

#2

Docket No. 1080.1088/JDH

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:

Yusuke KAWASAKI, et al.

Group Art Unit: To Be Assigned

Serial No.: To Be Assigned

Examiner: To Be Assigned

Filed: December 18, 2000

JCS15 U.S. PTO
09/739839
12/20/00

For: PROCESSING APPARATUS AND INTEGRATED CIRCUIT

**SUBMISSION OF CERTIFIED COPY OF PRIOR FOREIGN
APPLICATION IN ACCORDANCE
WITH THE REQUIREMENTS OF 37 C.F.R. § 1.55**

*Assistant Commissioner for Patents
Washington, D.C. 20231*

Sir:

In accordance with the provisions of 37 C.F.R. § 1.55, Applicants submit herewith a certified copy of the following foreign application:

Japanese Patent Application No. 2000-212815, filed July 13, 2000.

It is respectfully requested that Applicants be given the benefit of the foreign filing date, as evidenced by the certified papers attached hereto, in accordance with the requirements of 35 U.S.C. § 119.

Respectfully submitted,
STAAS & HALSEY LLP

Dated: December 18, 2000

By: _____

James D. Halsey, Jr.
Registration No. 22,729

700 Eleventh Street, N.W.
Suite 500
Washington, D.C. 20001
(202) 434-1500

日本国特許庁
PATENT OFFICE
JAPANESE GOVERNMENT

#2
Jc815 U.S. PTO
09/739839



別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: 2000年 7月13日

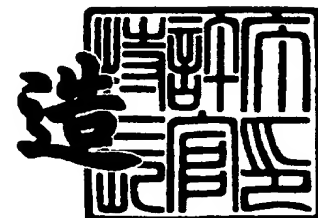
出願番号
Application Number: 特願2000-212815

出願人
Applicant(s): 富士通株式会社

2000年10月13日

特許庁長官
Commissioner,
Patent Office

及川耕造



出証番号 出証特2000-3084619

【書類名】 特許願

【整理番号】 0051226

【提出日】 平成12年 7月13日

【あて先】 特許庁長官殿

【国際特許分類】 G06F 9/00
G09C 1/00

【発明の名称】 処理装置および集積回路

【請求項の数】 20

【発明者】

 【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

 【氏名】 川▲崎▼ 雄介

【発明者】

 【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

 【氏名】 櫻井 博

【発明者】

 【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

 【氏名】 橋本 繁

【発明者】

 【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

 【氏名】 山本 浩憲

【特許出願人】

 【識別番号】 000005223

 【氏名又は名称】 富士通株式会社

【代理人】

 【識別番号】 100094330

【弁理士】

【氏名又は名称】 山田 正紀

【選任した代理人】

【識別番号】 100109689

【弁理士】

【氏名又は名称】 三上 結

【手数料の表示】

【予納台帳番号】 017961

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9912909

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 処理装置および集積回路

【特許請求の範囲】

【請求項 1】 プログラムを実行する CPU と、各所定の作用を成す 1 つ以上の内部デバイスと、前記 CPU と前記内部デバイスとを結ぶとともに外部にまで延びアドレスおよびデータを伝達するバスラインとを含む内部回路、および

前記バスラインの、外部に延びた部分に外付けされた、各所定の作用を成す 1 つ以上の外部デバイスを含む外部回路を備え、

前記内部回路が、前記バスラインの、外部への出入口に介在し、該バスライン上のアドレスおよびデータを、前記 1 つ以上の外部デバイス全体に割り当てられたアドレス空間を複数に分けた各領域に応じた各暗号化パターンで暗号化する暗号化部を含むものであることを特徴とする処理装置。

【請求項 2】 前記外部回路が複数の外部デバイスを含むものであり、

前記暗号化部は、前記複数の外部デバイスそれぞれに応じた暗号化パターンで暗号化するものであることを特徴とする請求項 1 記載の処理装置。

【請求項 3】 前記暗号化部は、前記外部回路がアクセスされていないタイミングで、前記バスラインの、外部に延びた部分に、ダミーのアドレスおよびデータを出力するものであることを特徴とする請求項 1 記載の処理装置。

【請求項 4】 前記 CPU は、クロックの供給を受け供給されたクロックに同期してプログラムを実行するものであるとともに、前記暗号化部も、クロックの供給を受け供給されたクロックに同期して暗号化を行なうものであって、

前記暗号化部に、前記 CPU に供給されるクロックよりも高速なクロックを供給するクロック供給部を備えたことを特徴とする請求項 1 記載の処理装置。

【請求項 5】 前記外部回路の構成を認識し、その構成に応じて、前記暗号化部における暗号化パターンを決定する暗号化パターン決定手段を有することを特徴とする請求項 1 記載の処理装置。

【請求項 6】 前記暗号化部は、前記バスライン上のアドレスおよびデータを、前記 1 つ以上の外部デバイス全体に割り当てられたアドレス空間を複数に分けた各領域に応じるとともに前記 CPU で実行されるアプリケーションプログラ

ムにも応じた暗号化パターンで暗号化するものであることを特徴とする請求項 1 記載の処理装置。

【請求項 7】 前記バスラインの、外部に延びた部分に接続され、該バスライン上の暗号化されたアドレスおよびデータを暗号化前のアドレスおよびデータに戻す逆暗号化部を備えたことを特徴とする請求項 1 記載の処理装置。

【請求項 8】 前記 1 つ以上の外部デバイス全体に割り当てられたアドレス空間を複数に分けた複数の領域のうちのいずれかの領域について、所定の初期化動作の都度暗号化パターンを変更する暗号化パターン変更手段を有することを特徴とする請求項 1 記載の処理装置。

【請求項 9】 前記暗号化部は、前記 1 つ以上の外部デバイス全体に割り当てられたアドレス空間を複数に分けた複数の領域のうちのいずれかの領域について、暗号化後のデータがアドレスに応じて変化する暗号化パターンを採用して、データを暗号化するものであることを特徴とする請求項 1 記載の処理装置。

【請求項 10】 プログラムを実行する CPU と、各所定の作用を成す 1 つ以上の内部デバイスと、前記 CPU と前記内部デバイスとを結ぶとともに外部にまで延びアドレスおよびデータを伝達するバスラインとを含む内部回路、および

前記バスラインの、外部に延びた部分に外付けされた、情報を記憶するメモリを含む外部回路を備え、

前記内部回路が、前記メモリに記憶された情報のうちの少なくとも一部の情報を、所定の初期化動作で暗号化して書き換える情報書換手段を有するものであることを特徴とする処理装置。

【請求項 11】 前記情報書換手段は、乱数を発生させ、発生させた乱数を用いた暗号化パターンを採用して暗号化を行なうものであることを特徴とする請求項 10 記載の処理装置。

【請求項 12】 前記メモリに記憶された情報のうちの少なくとも一部の情報が、前記所定の初期化動作を実行する以前において既に暗号化されたものであって、

前記情報書換手段は、該少なくとも一部の情報を一旦暗号化前の情報に戻し異なる暗号化パターンを採用して再度暗号化を行なって書き換えるものであること

を特徴とする請求項 1 0 記載の処理装置。

【請求項 1 3】 前記内部回路が前記暗号化部で採用される暗号化パターンを保持してなるものであって、

タンパ検出を行なうタンパ検出部を備えるとともに、

前記タンパ検出部によるタンパ検出を受けて前記内部回路内に保持されていた暗号化パターンを破壊する暗号化パターン破壊手段を備えたことを特徴とする請求項 1 又は 1 0 記載の処理装置。

【請求項 1 4】 プログラムを実行する CPU と、各所定の作用を成す 1 つ以上の内部デバイスと、前記 CPU と前記内部デバイスとを結ぶとともに外部にまで延びて、外部に延びた部分に、各所定の作用を成す 1 つ以上の外部デバイスが外付けされる、アドレスおよびデータを伝達するバスラインと、該バスラインの、外部への出入口に介在し、該バスライン上のアドレスおよびデータを、該バスラインの、外部に延びた部分に外付けされた 1 つ以上の外部デバイス全体に割り当てられた空間を複数に分けた各領域に応じた各暗号化パターンで暗号化する暗号化部とが搭載されてなることを特徴とする集積回路。

【請求項 1 5】 前記バスラインの、外部に延びた部分に、複数の外部デバイスが外付けされた場合に、前記暗号化部は、前記複数の外部デバイスそれぞれに応じた暗号化パターンで暗号化するものであることを特徴とする請求項 1 4 記載の集積回路。

【請求項 1 6】 前記暗号化部は、前記外部回路がアクセスされていないタイミングで、前記バスラインの、外部に延びた部分に、ダミーのアドレスおよびデータを出力するものであることを特徴とする請求項 1 4 記載の集積回路。

【請求項 1 7】 前記 1 つ以上の外部デバイス全体に割り当てられたアドレス空間を複数に分けた複数の領域のうちのいずれかの領域について、所定の初期化動作の都度暗号化パターンを変更する暗号化パターン変更手段を有することを特徴とする請求項 1 4 記載の集積回路。

【請求項 1 8】 前記暗号化部は、前記 1 つ以上の外部デバイス全体に割り当てられたアドレス空間を複数に分けた複数の領域のうちのいずれかの領域について、暗号化後のデータがアドレスに応じて変化する暗号化パターンを採用して

データを暗号化するものであることを特徴とする請求項 1 4 記載の集積回路。

【請求項 1 9】 プログラムを実行する CPU と、各所定の作用を成す 1 つ以上の内部デバイスと、前記 CPU と前記内部デバイスとを結ぶとともに外部にまで延びて、外部に延びた部分に、情報を記憶するメモリが外付けされる、アドレスおよびデータを伝達するバスラインとを備えるとともに、

前記メモリに記憶された情報のうちの少なくとも一部の情報を、所定の初期化動作で暗号化して書き換える情報書換手段を有するものであることを特徴とする集積回路。

【請求項 2 0】 前記情報書換手段は、乱数を発生させ、発生させた乱数を用いた暗号化パターンを採用して暗号化を行なうものであることを特徴とする請求項 1 9 記載の集積回路。

【発明の詳細な説明】

【0 0 0 1】

【発明の属する技術分野】

本発明は、CPU および内部デバイスを有する内部回路と、その内部回路に対し外付けされた外部デバイスを含む外部回路とを備えた処理装置、および、CPU および内部デバイスが搭載されるとともに外部デバイスの外付けが可能な集積回路に関する。

【0 0 0 2】

【従来の技術】

近年の L S I 技術の発達により、プログラムを実行する CPU や、その CPU で実行されるプログラムが格納されるメモリや、さらに他の様々なデバイスを 1 つのチップ上に集積することができるようになり、装置の小型化、低コスト化等に大きく貢献している。このような L S I を製造するにあたり、ユーザによらず同一のプログラムを実行するシステムであって、かつ完成したあと途中でプログラムを変更する必要がないシステムについては L S I チップ上にプログラムを記憶したメモリを搭載しておけばよいが、ユーザに応じて異なるプログラムを実行させたり、あるいは、使用している途中でプログラムを変更する必要がある場合、上記のような構成の L S I にさらに外部メモリを外付けすることができるよう

に構成しておき、使用している途中で変更する可能性のあるプログラム、あるいはユーザに応じて異なるプログラムはその外付けの外部メモリに記憶するようにしておくことが望ましい。

【0003】

【発明が解決しようとする課題】

ところが、そのような外部メモリを外付けることができるシステムの場合、その外部メモリの内容が不正に書き換えられたり、あるいはその外部メモリが、その外部メモリと同一仕様の、不正なプログラムを記憶したメモリに差し替えられてしまい、内部のメモリに記憶されている重要なプログラムやデータが不正にアクセスされ、その重要なプログラムやデータの内容が不正に解読されてしまう危険性がある。以下に、一例を挙げる。

【0004】

近年、急速に現金価値や現金相当のポイント価値をデータとしてもつＩＣカードや磁気カードが普及しつつあり、それに伴って、カードの偽造や変造を防止するための対策としてデータのセキュリティ確保が急務となってきている。これに対処するために、過去においても装置の逆解析（リバースエンジニアリング）を防ぐ方法が試みられてきたが、それらの試みにもかかわらず裏ＲＯＭ等が作成され、装置が開発者の不本意な用途に悪用されることが絶えないのが現状である。

【0005】

本発明は、上記事情に鑑み、不正なアクセスや逆解析の防止が図られた処理装置および集積回路を提供することを目的とする。

【0006】

【課題を解決するための手段】

上記目的を達成する本発明の処理装置のうちの第１の処理装置は、

プログラムを実行するＣＰＵと、各所定の作用を成す１つ以上の内部デバイスと、ＣＰＵと内部デバイスとを結ぶとともに外部にまで延びアドレスおよびデータを伝達するバスラインとを含む内部回路、および

上記バスラインの、外部に延びた部分に外付けされた、各所定の作用を成す１つ以上の外部デバイスを含む外部回路を備え、

上記内部回路が、上記バスラインの、外部への出入口に介在し、そのバスライン上のアドレスおよびデータを、上記の1つ以上の外部デバイス全体に割り当てられたアドレス空間を複数に分けた各領域に応じた各暗号化パターンで暗号化する暗号化部を含むものであることを特徴とする。

【0007】

ここで、上記暗号化部で採用される暗号化パターンには、アドレスおよびデータの双方とも暗号化しないことも1つの暗号化パターンとして含まれる。

【0008】

このように、アドレス空間を複数に分割し、その分割した各領域ごとに異なったパターンで暗号化することにより、暗号化の解析が困難となる。

【0009】

上記本発明の第1の処理装置において、上記外部回路が複数の外部デバイスを含むものであり、

上記暗号化回路は、上記複数の外部デバイスそれぞれに応じた暗号化パターンで暗号化するものであることが好ましい。

【0010】

こうすることにより、例えば外部デバイスの1つとしてフラッシュROMを備えた場合は、そのフラッシュROMに関してはアドレスとデータとの双方を暗号化し、外部デバイスの1つとして連続アドレスについて高速読出しが可能なRAMについては性能を落とさないようにデータのみ暗号化するか、あるいはアドレスについても暗号化するものの、連続読出しの行なわれる、アドレスの下位ビット側は暗号化しないようにし、外部デバイスの1つとしてI/Oデバイスを備えた場合は、アドレス、データとも暗号化しないなど、その外部デバイスの性質に合わせた暗号化を行なうことができる。

【0011】

また、上記本発明の第1の処理装置において、上記暗号化部は、外部回路がアクセスされていないタイミングで、バスラインの、外部に延びた部分に、ダミーのアドレスおよびデータを出力するものであることが好ましい。

【0012】

こうすることにより不正な解析が一層難しくなる。

【 0 0 1 3 】

また、上記本発明の第 1 の処理装置において、上記 CPU は、クロックの供給を受け供給されたクロックに同期してプログラムを実行するものであるとともに、上記暗号化部も、クロックの供給を受け供給されたクロックに同期して暗号化を行なうものであって、上記暗号化部に、CPU に供給されるクロックよりも高速なクロックを供給するクロック供給部を備えることが好ましい。

【 0 0 1 4 】

こうすると、複雑な暗号化が可能になる。

【 0 0 1 5 】

さらに、上記本発明の第 1 の処理装置において、外部回路の構成を認識し、その構成に応じて、暗号化部における暗号化パターンを決定する暗号化パターン決定手段を有することが好ましい。

【 0 0 1 6 】

この暗号化パターン決定手段を持つことにより、外部回路の構成が異なるごとにオペレータがいちいち暗号化パターンを決定するといった作業が不要となる。

【 0 0 1 7 】

さらに、上記本発明の第 1 の処理装置において、上記暗号化部は、上記バスライン上のアドレスおよびデータを、上記の 1 つ以上の外部デバイス全体に割り当てられたアドレス空間を複数に分けた各領域に応じるとともに CPU で実行されるアプリケーションプログラムにも応じた暗号化パターンで暗号化することが好ましい。

【 0 0 1 8 】

これにより、暗号化のパターンが一層複雑となり、不正な解析が一層困難となる。

【 0 0 1 9 】

さらに、上記本発明の第 1 の処理装置において、上記バスラインの、外部に延びた部分に接続され、バスライン上の暗号化されたアドレスおよびデータを暗号化前のアドレスおよびデータに戻す逆暗号化部を備えることが好ましい。

【 0 0 2 0 】

この逆暗号化部を備えないままデバッグを行なおうとするとアドレスやデータが暗号化されているためデバッグが極めて困難になる。そこで、この逆暗号化部を備えることにより、装置の開発時に容易にデバッグを行なうことができる。

【 0 0 2 1 】

この逆暗号化部は、デバッグが済んだ後は不要であり、処理装置から取り外され、あるいは動作不能な状態に固定あるいは破壊されることが望ましい。

【 0 0 2 2 】

さらに、上記本発明の第 1 の処理装置において、上記の 1 つ以上の外部デバイス全体に割り当てられたアドレス空間を複数に分けた複数の領域のうちのいずれかの領域について、所定の初期化動作の都度暗号化パターンを変更する暗号化パターン変更手段を有することが好ましい。

【 0 0 2 3 】

所定の初期化動作、例えば電源投入時やリセット時等に暗号化パターンを再設定することにより、不正な解析が一層困難になり、セキュリティが一層向上する。

【 0 0 2 4 】

さらに、上記本発明の第 1 の処理装置において、上記暗号化部は、上記 1 つ以上の外部デバイス全体に割り当てられたアドレス空間を複数に分けた複数の領域のうちのいずれかの領域について、暗号化後のデータがアドレスに応じて変化する暗号化パターンを採用して、データを暗号化するものであることが好ましい。

【 0 0 2 5 】

このように、データを暗号化するときの暗号化関数としてアドレスの関数を採用することにより、複雑な暗号化が可能となり、不正な解析が一層困難となり、データのセキュリティが一層向上する。

【 0 0 2 6 】

また本発明の処理装置のうちの第 2 の処理装置は、

プログラムを実行する CPU と、各所定の作用を成す 1 つ以上の内部デバイスと、CPU と内部デバイスとを結ぶとともに外部にまで延びアドレスおよびデー

タを伝達するバスラインとを含む内部回路、および

上記バスラインの、外部に延びた部分に外付けされた、情報を記憶するメモリを含む外部回路を備え、

上記内部回路が、上記メモリに記憶された情報のうちの少なくとも一部の情報を、所定の初期化動作で暗号化して書き換える情報書換手段を有するものであることを特徴とする。

【0027】

ここで上記所定の初期化動作とは、典型的には、最初の電源投入時の初期化動作である。

【0028】

このように、例えば最初の電源投入時の初期化動作等、所定の初期化動作で、メモリの内容を暗号化して書き換えることにより、データのセキュリティが一層向上する。

【0029】

この場合に、上記情報書換手段は、乱数を発生させ、発生させた乱数を用いた暗号化パターンを採用して暗号化を行なうものであることが好ましい。

【0030】

この場合、処理装置のメーカ側の人間を含め、誰もが知らない暗号化パターンで情報が暗号化されることになり、データのセキュリティがさらに向上する。

【0031】

ここで、上記第2の処理装置において、上記メモリに記憶された情報のうちの少なくとも一部の情報が、上記の所定の初期化動作を実行する以前において既に暗号化されたものであって、

上記情報書換手段は、その少なくとも一部の情報を一旦暗号化前の情報に戻し異なる暗号化パターンを採用して再度暗号化を行なって書き換えるものであることも好ましい形態である。

【0032】

この場合に、上記の少なくとも一部の情報を暗号化前の情報に戻すための復号化情報が上記メモリに記憶されてなるものであって、

上記情報書換手段は、その少なくとも一部の情報を、その復号化情報を用いて一旦暗号化前の情報に戻すものであってもよい。

【 0 0 3 3 】

このように、工場出荷時には別の暗号化パターンで暗号化しておくことによりセキュリティがさらに向上する。

【 0 0 3 4 】

また、上記のように、工場出荷時に別の暗号化パターンで暗号化しておくにあたっては、上記の少なくとも一部の情報が公開鍵により暗号化されたものであるとともに、この処理装置は秘密鍵が埋め込まれてなるものであって、

上記情報書換手段は、その少なくとも一部の情報をその秘密鍵を用いて一旦暗号化前の情報に戻すものであってもよく、あるいは上記の少なくとも一部の情報を暗号化前の情報に戻すための、暗号化された形式の復号化情報を外部より取得する情報取得部を備え、

上記情報書換手段は、情報取得部で取得された、暗号化された形式の復号化情報を復号化して平文の復号化情報を取り出しこの平文の復号化情報を用いて上記の少なくとも一部の情報を一旦暗号化前の情報に戻すものであってもよい。

【 0 0 3 5 】

暗号化パターンとして公開鍵を用い、その公開鍵で暗号化された情報をメモリに書き込んでおき、内部に埋め込まれた秘密鍵で暗号化前の情報に戻すようにすると、例えば同一仕様の処理装置を複数の会社等で使用した場合に、各会社に公開鍵のみを渡すことにより、会社間のセキュリティが確保できる。

【 0 0 3 6 】

また、復号化情報を外部より取得できるように構成すると、例えば通信等により鍵管理センター等から復号化情報を入手することが可能となり、柔軟なシステム構成が可能となる。

【 0 0 3 7 】

さらに、上記第 2 の処理装置において、上記内部回路が上記暗号化部で採用される暗号化パターンを保持してなるものであって、

タンパ検出を行なうタンパ検出部を備えるとともに、

上記タンパ検出部によるタンパ検出を受けて上記内部回路内に保持されていた暗号化パターンを破壊する情報破壊手段を備えることが好ましい。

【 0 0 3 8 】

この処理装置を不正にこじ開けたり分解しようとしたときにタンパ検出がなされ、そのタンパ検出を受けて暗号化パターンを破壊することにより、不正な解読がますます困難になり、セキュリティの一層の向上に寄与することになる。

【 0 0 3 9 】

また、上記目的を達成する本発明の集積回路のうちの第 1 の集積回路は、プログラムを実行する CPU と、各所定の作用を成す 1 つ以上の内部デバイスと、CPU と内部デバイスとを結ぶとともに外部にまで延びて、外部に延びた部分に、各所定の作用を成す 1 つ以上の外部デバイスが外付けされる、アドレスおよびデータを伝達するバスラインと、そのバスラインの、外部への出入口に介在し、そのバスライン上のアドレスおよびデータを、そのバスラインの、外部に延びた部分に外付けされた 1 つ以上の外部デバイス全体に割り当てられた空間を複数に分けた各領域に応じた各暗号化パターンで暗号化する暗号化部とが搭載されてなることを特徴とする。

【 0 0 4 0 】

本発明の第 1 の集積回路は、上記の構成を有するものであり、本発明の第 1 の処理装置と同一の作用効果を奏するとともに、集積回路（LSI）であることからその回路構成等の解析が困難であり、この点からもセキュリティの向上に寄与している。

【 0 0 4 1 】

ここで、上記第 1 の集積回路において、上記の本発明の第 1 の処理装置と同様、上記暗号化部で採用される暗号化パターンには、典型的には、アドレスおよびデータの双方とも暗号化しないことも 1 つの暗号化パターンとして含まれており、また、上記バスラインの、外部に延びた部分に、複数の外部デバイスが外付けされた場合に、暗号化部は、それら複数の外部デバイスそれぞれに応じた暗号化パターンで暗号化するものであることが好ましく、

また、上記暗号化部は、外部回路がアクセスされていないタイミングで、上記

バスラインの、外部に延びた部分に、ダミーのアドレスおよびデータを出力するものであることも好ましい形態であり、

さらに、上記 1 つ以上の外部デバイス全体に割り当てられたアドレス空間を複数に分けた複数の領域のうちのいずれかの領域について、所定の初期化動作の都度暗号化パターンを変更する暗号化パターン変更手段を有することも好ましい形態であり、

さらに、上記暗号化部は、上記 1 つ以上の外部デバイス全体に割り当てられたアドレス空間を複数に分けた複数の領域のうちのいずれかの領域について、暗号化後のデータがアドレスに応じて変化する暗号化パターンを採用して、データを暗号化するものであることも好ましい形態である。

【 0 0 4 2 】

また、本発明の集積回路のうちの第 2 の集積回路は、プログラムを実行する CPU と、各所定の作用を成す 1 つ以上の内部デバイスと、CPU と内部デバイスとを結ぶとともに外部にまで延びて、外部に延びた部分に、情報を記憶するメモリが外付けされる、アドレスおよびデータを伝達するバスラインとを備えるとともに、上記メモリに記憶された情報のうちの少なくとも一部の情報を、所定の初期化動作で暗号化して書き換える情報書換手段を有するものであることを特徴とする。

【 0 0 4 3 】

本発明の第 2 の集積回路は、上記の構成を有するものであり、本発明の第 1 の処理装置と本発明の第 1 の集積回路との関係と同様、本発明の第 2 の処理装置と同一の作用効果を奏するものであり、さらに集積回路（LSI）であることからその回路構成等の解析が困難であり、この点からもセキュリティの向上が図られている。

【 0 0 4 4 】

ここで、上記第 2 の集積回路において、上記本発明の第 2 の処理装置と同様、上記所定の初期化動作は、典型的には、最初の電源投入時の初期化動作であり、

また、上記情報書換手段は、乱数を発生させ、発生させた乱数を用いた暗号化パターンを採用して暗号化を行なうものであることが好ましく、

さらに、上記メモリに記憶された情報のうちの少なくとも一部の情報が、上記の所定の初期化動作を実行する以前において既に暗号化されたものであって、

上記情報書換手段は、その少なくとも一部の情報を一旦暗号化前の情報に戻し異なる暗号化パターンを採用して再度暗号化を行なって書き換えるものであることも好ましい形態である。

【 0 0 4 5 】

尚、本発明においては、1つの暗号化演算方式を本発明にいう暗号化パターンの1つとしてとらえ、暗号化演算方式が異なることをもって暗号化パターンが異なるものとしてもよく、暗号化演算方式は共通であって、その暗号化演算方式において用いられる変数等が異なることをもって暗号化パターンが異なるものとしてもよい。

【 0 0 4 6 】

【発明の実施の形態】

以下、本発明の実施形態について説明する。

【 0 0 4 7 】

図1は、本発明の処理装置の第1実施形態を示すブロック図である。

【 0 0 4 8 】

この図1に示す処理装置1は、LSI10の内部に搭載された内部回路100と、LSI10の外部に外付けされた外部回路200と、その他発振器301、302等から構成されている。このLSI10は、本発明の集積回路の一実施形態にも相当する。

【 0 0 4 9 】

LSI10の内部に構成された内部回路100は、中央処理装置(CPU)101、および、それぞれが、本発明にいう内部デバイスである、内部メモリ102、暗号化情報レジスタ103、アドレスデコーダ104、およびその他の周辺回路105を有する。CPU101および各種の内部デバイスは、バスライン110で相互に接続されている。このバスラインは、アドレスバス111とデータバス112とで構成され、LSI10の外部にまで延びている。このバスライン110の、外部にまで延びた部分110aには、各種の外部デバイスが接続され

ている。外部デバイスについて後述する。

【 0 0 5 0 】

L S I 1 0 の内部に構成された内部回路 1 0 0 には、さらにバスライン 1 1 0 の、外部への出入り口に介在するように、暗号化部 1 2 0 が備えられている。この暗号化部 1 2 0 は、暗号化回路 1 2 1、バスインターフェース 1 2 2、および乱数発生回路 1 2 3 から構成されている。

【 0 0 5 1 】

C P U 1 0 1 には、発振器 3 0 1 からのクロック信号が入力され、C P U 1 0 1 は、その発振器 3 0 1 から受けたクロック信号に同期して各種のプログラムを実行する。

【 0 0 5 2 】

また、暗号化回路 1 2 1 には、C P U 1 0 1 に入力されるクロック信号よりも繰り返し周波数の高いクロック信号を発生するもう 1 つの発振器 3 0 2 からのクロック信号が入力され、暗号化回路 1 2 1 は、その発振器 3 0 2 からの繰り返し周波数の高いクロック信号に同期して暗号化処理が行なわれる。暗号化処理の詳細については後述する。

【 0 0 5 3 】

上記の 2 つの発振器 3 0 1、3 0 2 は、相互に同期したクロック信号を発生するものであり、したがって、共通の発振源で得られた高速クロックを分周して各クロック信号を生成するものであってもよい。

【 0 0 5 4 】

また、バスライン 1 1 0 の、外部に延びる部分 1 1 0 a には、複数の外部デバイス、すなわち、この図 1 に示す例では、液晶表示装置 (L C D) 2 0 1、キーボード (K B) 2 0 2、読出専用メモリ (R O M) 2 0 3、フラッシュ R O M 2 1 1、ランダムアクセスメモリ (R A M) 2 1 2 が接続されている。また、この図 1 には、この図 1 に示す L S I 1 0 と同一の構成をもつもう 1 つの L S I 等、内部回路 1 0 0 と同様の暗号化機構を持つデバイス 2 1 3 も接続されており、さらに、C P U 1 0 1 で動作するプログラムのデバッグのための逆暗号化回路 2 1 4 も接続されている。デバイス 2 1 3 および逆暗号化回路 2 1 4 は、それらの説

明のためにこの図1と一緒に示したものであるが、デバイス213は、LSI10と、そのLSI10と同様な構成を持つデバイス213との間で暗号化通信を行なう場合に接続されるものであり、逆暗号化回路214はプログラムのデバッグのためのものであってデバッグ終了後は取り外されるものである。

【0055】

ここで、LCD201、KB202、および、この図1に示す実施形態においてはROM203も、アドレスおよびデータの双方について暗号化を行なわない外部デバイスに属し、一方、フラッシュROM211およびRAMは、アドレスあるいはデータに関し暗号化を行なってアクセスする外部デバイスに属する。ここでは、フラッシュROM211は、データのみ暗号化され、RAMは、アドレスとデータの双方について暗号化される。また、デバイス213もアドレスおよびデータの双方について暗号化されてLSI10との間で暗号化通信が行なわれる。また、逆暗号化回路214が接続されるときは、この逆暗号化回路214は、本実施形態ではアドレスおよびデータの双方について暗号化を行なわないデバイスに属する。

【0056】

ここで、バスライン110は、CPU101に接続された部分（この部分のアドレス、データをそれぞれA1、D1と表記する）と、暗号化回路121とバスインターフェース122とに挟まれた部分（この部分のアドレス、データをそれぞれA2、D2と表記する）と、さらに、LSI10の外部に延びた部分110a（この部分のアドレス、データをそれぞれA3、D3と表記する）とに分かれている。

【0057】

図2は、図1に示す処理装置のメモリマップを示す図である。

【0058】

外部デバイスの1つであるフラッシュROMには、複数のアプリケーションプログラムが格納されており、内部デバイスの1つである内部メモリにはOSプログラムが格納されている。また、外部デバイスの1つであるROMには、この処理装置の装置構成情報、例えば接続されている外部デバイスの種類やメモリ容量

等が記録されている。

【 0 0 5 9 】

図 3 は、図 1 に示す処理装置に電源が投入されたときに実行される初期化プログラムのフローチャートである。この初期化プログラムは、OS プログラムの一種として内部メモリ 1 0 2 に格納されており、電源投入時に CPU 1 0 1 で実行される。

【 0 0 6 0 】

図 3 に示す初期化プログラムでは、先ず外部デバイスの 1 つである ROM 2 0 3 に格納された装置構成情報が読み出され（ステップ a 1）、その情報に基づいて、図 2 に示すようなメモリマップが作成されるとともに、そのメモリマップの各エリアについて暗号化パターンが決定される（ステップ a 2）。但し、アドレスもデータも暗号化しないということも、この暗号化パターンの 1 つとして含まれている。

【 0 0 6 1 】

この初期化プログラムでは、その後、その他の諸々の初期化処理が行なわれる（ステップ a 3）。

【 0 0 6 2 】

図 1 に戻って説明を続行する。

【 0 0 6 3 】

CPU 1 0 1 は、アドレス A 1 およびデータ D 1 を用いて情報のリード、ライトを行なう。一方外部デバイスは、暗号化の必要なデバイスであるか暗号化は不要な（あるいは暗号化は禁止される）デバイスであるかに関わらず、アドレス A 3 およびデータ D 3 を用いてアクセスされる。

【 0 0 6 4 】

CPU 1 0 1 は、外部デバイスへのアクセスの前に、図 2 に示すメモリマップ上の、暗号化を行ないたいエリア（暗号化エリア）の領域情報と各暗号化エリアに対する暗号化パターンを、暗号化情報レジスタ 1 0 3 に書き込んでおく。

【 0 0 6 5 】

アドレスデコーダ 1 0 4 は、アドレス A 1 を入力するとともに暗号化情報レジ

スタ103から暗号化を行なうエリアを示す領域情報を受けとって、アクセス対象のデバイスに対し、チップセレクト信号CS0～SC6を出力するとともに、暗号化回路121に対し、どのデバイスがアクセス対象となっており暗号化が必要であるか否かを示す暗号化制御信号Crpを出力する。

【0066】

暗号化回路121は、アドレスデコーダから暗号化制御信号Crpを受け取り、暗号化情報レジスタ103に記録されている暗号化パターンの情報を元に、アドレスA1、データD1について暗号化を行なう必要があるときにその暗号化エリアに応じた暗号化を行ない、アドレスA2、データD2を出力する。これらのアドレスA2、データD2は、バスインタフェース123を経由しアドレスA3、データD3としてLSI10の外部に出力される。

【0067】

CPU101からバスインタフェース122には、外部デバイスをアクセス対象としているか否かを示す外部バスアクセス信号が伝達され、バスインタフェース122は、外部デバイスのアクセスが要求されているときは暗号化回路121から出力されたアドレスA2、データD2を外部のアドレスA3、データD3として外部に出力し、外部デバイスのアクセス要求がないときは、乱数発生回路123からの乱数を基に、ダミーのアドレス、データを生成して、外部のアドレスA3、データD3として出力する。このようにダミーのアドレス、データを出力することにより、不正な解析を一層困難にしている。

【0068】

尚、ここでは、内部から外部へのアドレス、データの変換について述べたが、外部のフラッシュメモリ211やRAM212、ROM203等から読み出されたデータD3については、バスインタフェース122はデータD2として内部に取り込み、そのデータが暗号化されたデータであるときは、暗号化回路121でその暗号化に対する復号化が行なわれ、暗号化前のデータD1として、CPU101等に伝達される。

【0069】

ここで、本実施形態においては暗号化パターンとして、アドレスもデータも暗

号化しないという暗号化パターンのほか、例えば、

(1) タイプ1

$$A3 = A1 \text{ XOR } p1$$

$$D3 = D1 \text{ XOR } p1$$

(2) タイプ2

$$A3 = A1$$

$$D3 = A1 + D1 + p1$$

(3) タイプ3

タイプ2の演算結果としてのデータについて、さらにそのデータの上位と下位を入れ替える

という暗号化パターンが採用される。

【0070】

ここで、上記 $p1$ は、例えば乱数等により得られた適当な定数であり、

$A \text{ XOR } B$ は、 A と B の対応する各ビットごとの排他論理和演算を行なうことを意味し、 $A + B$ は、 A 、 B を数値とみたときの加算演算を意味している。

【0071】

図3を参照して説明したように、電源投入時の初期化動作において、CPU101は、外部デバイスの1つであるROM203に格納された装置構成情報を読み出し、図2に示すようなメモリマップを作成するとともに、暗号化エリアについて暗号化パターンを決定するが、ここでは一例として、フラッシュROM211については、アドレスについては暗号化は行なわずにデータについてのみ暗号化を行なう、例えば上記の(2)の暗号化パターンが採用され、RAM212についてはアドレスおよびデータの双方について暗号化を行なう、例えば上記の(1)の暗号化パターンが採用される。

【0072】

ここで、RAM212については、上記(1)のタイプ1の暗号化パターンが採用されているため、例えば $p1 = 0x5555$ (0xはそれに続く'5555'が16進数であることを意味する) であるとする、

$$\begin{aligned}
 &A3 (0x5455) \\
 &= A1 (0x0100) \quad \text{XOR} \quad p1 (0x5555) \\
 &D3 (0x5476) \\
 &= D1 (0x0123) \quad \text{XOR} \quad p1 (0x5555)
 \end{aligned}$$

のように、アドレス及びデータとも、もとのアドレス、データとは全く異なる値となる。

【0073】

また、フラッシュROM211については、上記(2)タイプ2の暗号化パターンが採用されており、 $p1 = 0x5555$ であるとする、

$$\begin{aligned}
 &A3 (0x0100) = A1 (0x0100) \\
 &D3 (0x5778) \\
 &= A1 (0x0100) + D1 (0x0123) + p1 (0x5555)
 \end{aligned}$$

のように、アドレスは変更されず、データについてはもとのデータとは全く異なる値となる。ここでは、データを暗号化するにあたり、アドレスA1の関数としているため、同一のデータD1であってもアドレスA1に応じて暗号化後のデータD3が異なることになり、不正な解析を一層困難にし、セキュリティの一層の向上が図られている。

【0074】

尚、上記は暗号化パターンの計算上の例を挙げたものであり、アドレスを暗号化する場合、その暗号化対象のデバイスのアドレスエリアを越えて他のデバイスのアドレスエリアに移らないようにその暗号化のアルゴリズム上考慮されている。

【0075】

また、例えば、同一のRAM212であっても、CPU101で実行されるアプリケーションプログラムに応じてRAM212をアクセスするときの暗号化パターンを変更してもよい。そのようにメモリエリア（アクセスされる外部デバイス）に応じて暗号化パターンを選択するだけでなく、同一のメモリエリア（同一の外部デバイス）であっても、アプリケーションプログラムに応じて暗号化パターンを変更すると、バスライン110の、外部に延びた部分110aに出力さ

れるアドレスやデータが一層複雑に暗号化されたものとなり、不正な解析がさらに困難となり、セキュリティの一層の向上が図られる。

【0076】

ここで、CPU101と暗号化回路121が仮に同一のクロックで動作していると、暗号化回路121では複雑な暗号化演算を行なうことができないことになる。例えばCPU101が1クロック毎に外部へアクセスを行なうとすると暗号化回路121は1クロック以内に暗号化処理を終える必要がある。例えば上述の(3)のタイプ3の暗号化処理の場合、(2)のタイプ2の暗号化を行なうのに1クロック分の時間を要し、さらに上位と下位を入れ替えるのに1クロック分の時間を要し、合計2クロック分の時間を要するものとする、暗号化回路121で1クロック以内に暗号化処理を終える必要がある場合、この(3)のタイプ3の暗号化パターンは採用することができないことになる。

【0077】

図1に示す実施形態の場合、CPU101にクロックを供給する発振器301よりも高速なクロックを生成する発振器302を備え、暗号化回路121は発振器302から供給された高速なクロックに同期して動作するため、複数クロック必要とする、例えば上述の(3)のタイプ3の暗号化パターンや、さらに複雑な暗号化パターンを採用することができる。

【0078】

例えばCPU101には、10MHzのクロックが供給されており、暗号化回路121に100MHzのクロックが供給されていると、暗号化回路では10クロックを使って暗号化処理を行なうことができる。

【0079】

また、図1に示す処理装置の内部回路100はLSI10の内部に作り込まれたものであり、そのLSI10からは、暗号化回路121及びバスインタフェース122を経由して暗号化されたアドレスやデータが出力され、このままでは、このLSI10を用いた製品を開発する際、CPU101で実行されるプログラムのデバッグが極めて困難となる。そこで、図1に示す処理装置には、逆暗号化回路214が接続されている。

【 0 0 8 0 】

この逆暗号化回路 2 1 4 には、デバッグに先立って、CPU 1 0 1 から、暗号化情報レジスタ 1 0 3 に書き込む内容と同様の内容の、暗号化パターン及び暗号化エリアの情報が書き込まれ、逆暗号化回路 2 1 4 は、その後のデバッグにおいて、前もって書き込まれた暗号化パターンや暗号化エリアの情報に基づいて、バスライン 1 1 0 の、外部に延びた部分 1 1 0 a に出力された、暗号化されたアドレスやデータを復号化して、暗号化前のアドレスやデータを復元する。こうすることにより、その逆暗号化回路 2 1 4 により復元されたアドレスやデータを例えば計測器でもニタし、CPU 1 0 1 で実行されるプログラムのデバッグを容易に行なうことができる。

【 0 0 8 1 】

この逆暗号化回路 2 1 4 は、このままにしておくと、不正な解析を困難にする目的でアドレスやデータを暗号化したことの意味を失うことになるため、別装置として構成しておいて、デバッグ終了後は取り外される。あるいは、そこに付けたまま完全に動作不能としてもよい。

【 0 0 8 2 】

また、図 1 には、LSI 1 0 と同様の暗号化機構をもつデバイス 2 1 3 が接続されている。このように、この LSI 1 0 を複数組み合わせると、基板上での LSI 同士の暗号化通信を行なうことも可能となる。

【 0 0 8 3 】

図 4 は、本発明の処理装置の第 2 実施形態のブロック図である。

【 0 0 8 4 】

この図 4 に示す処理装置 5 は、LSI 5 0 の内部に組み込まれた内部回路 5 0 0 と LSI 5 0 の外部に外付けされた外部回路 6 0 0 とから構成されている。LSI 5 0 は、本発明の集積回路の一実施形態にも相当する。

【 0 0 8 5 】

LSI 5 0 内に作り込まれた内部回路 5 0 0 は、CPU 5 0 1、内部メモリ 5 0 2、アドレスバススクランブル演算回路 5 0 3、アドレスバススクランブルパターンメモリ 5 0 4、データバススクランブル演算回路 5 0 5、データバススク

ランブルパターンメモリ 506、およびデコーダ回路 507 を有し、それらはバスライン 510 で相互に接続されている。このバスライン 510 はアドレスバス 511 とデータバス 512 とからなる。内部回路 500 には、その他の内部デバイスも備えられているから、それらの図示及び説明は省略する。

【0086】

L S I 10 内に作り込まれた内部回路 500 の、図 4 に示す構成要素のうち、CPU 501 および内部メモリ 502 を除く構成要素の複合、すなわち、アドレスバススクランブル演算回路 503、アドレスバススクランブルパターンメモリ 504、データバススクランブル演算回路 505、データバススクランブルパターンメモリ 506、およびデコーダ回路 507 の複合が、本発明にいう暗号化部の一例に相当する。

【0087】

また、バスラインの、L S I 50 の外部に延びた部分には、外部回路 600 を構成する RAM 601 とフラッシュ ROM 602 が接続されている。

【0088】

内部回路 500 を構成する内部メモリ 502 には OS プログラムが格納されており、また、外部回路 500 を構成するフラッシュ ROM 602 にはアプリケーションプログラムが格納されており、内部回路 500 の CPU 501 ではそれら各種のプログラムが実行される。また、外部回路 600 を構成する RAM 601 には、各種のデータが読み書き自在に格納される。

【0089】

また、アドレスバススクランブル演算回路 503 およびデータバススクランブル演算回路 505 は、それぞれ、アドレス A0 ～ 15 およびデータ D0 ～ 7 をスクランブル（暗号化）する演算回路であり、アドレスバススクランブルパターンメモリ 504 およびデータバススクランブルパターンメモリ 506 には、それぞれアドレスバススクランブル演算回路 503 およびデータバススクランブル演算回路 505 におけるスクランブル演算において用いられるスクランブルパターンが格納されている。これらのアドレスバススクランブルパターンメモリ 504 およびデータバススクランブルパターンメモリ 506 は、不揮発性メモリ等により

構成されており、装置の電源が切断されても内容を保持することが可能であり、また、CPU501により、スクランブルパターンの書き換えが可能である。

【0090】

本実施形態では、アドレスバススクランブル演算回路503およびデータバススクランブル演算回路505のいずれにも、排他的論理和回路が採用されている。

【0091】

図5は、排他的論理和回路を示す図である。

【0092】

図5に示す排他的論理和回路（図4に示すアドレスバススクランブル演算回路503あるいはデータバススクランブル演算回路506）には、バスライン510を經由して入力IN（アドレスA0～15あるいはデータD0～7）が入力されるとともに、アドレスバススクランブルパターンメモリ504あるいはデータバススクランブルパターンメモリ506から、スクランブルパターンSP（SPA0～15あるいはSPD0～7）が入力され、出力OUT（SA0～15あるいはSP0～7）として、

$$OUT = IN \quad XOR \quad SP \quad \dots (1)$$

但し、XORは排他的論理和を表わす
が出力される。

【0093】

ここで、スクランブルパターンSPを全ビットとも0にすることにより、スクランブルを禁止することができ、また一部のビットを0にすることにより、対応するビットのスクランブルを禁止することができる。例えば16ビットのスクランブルパターンSPのうち下位4ビットを常に0にすると、下位4ビットについてはスクランブル（暗号化）が行なわれないことになる。

【0094】

本実施形態におけるアドレスバススクランブル演算回路503およびデータバススクランブル演算回路505（以下、これらを総称するときは、単に、スクランブル演算回路と称する）には、上記（1）式に基づく演算を行なう排他的論理

和回路が採用されているが、以下に、スクランブル演算回路として採用することのできる各種の回路構成を例示しておく。

【 0 0 9 5 】

図 6 ～ 図 9 は、スクランブル演算回路として採用することのできる各回路構成を示した図である。

【 0 0 9 6 】

図 6 に示すスクランブル演算回路には、加算回路が採用されており、ここでは

$$OUT = IN + SP \quad \dots (2)$$

の演算が行なわれる。

【 0 0 9 7 】

図 7 には、加算回路と排他的論理和回路が示されており、

ここでは、

$$OUT = (IN + SP1) \text{ XOR } SP2 \quad \dots (3)$$

但し、SP 1, SP 2 は、相互に異なる、あるいは同一の 2 つのスクランブルパターンである。

の演算が行なわれる。

【 0 0 9 8 】

また、図 8 には、排他的論理和回路とビット入換回路が示されており、ここでは、

$$OUT = (IN \text{ XOR } SP)_m \quad \dots (4)$$

(排他的論理和演算を行なった後上位と下位のビットを m ビット分入れ換える)

の演算が行なわれる。

【 0 0 9 9 】

さらに、図 9 には、加算回路と排他的論理和回路が示されており、ここでは、

$$OUT = (IN (\text{データ}) + IN (\text{アドレス})) \text{ XOR } SP \quad \dots (5)$$

但し、IN (データ) は、データバス上のデータ、IN (アドレス) はアドレスバス上のアドレスである。

の演算が行なわれる。但し、この (5) 式に基づく演算は、データバススクラン

ブル演算回路 5 0 5 として採用可能なものであり、データをスクランブルするにあたりアドレスを用いると、不正な解析が一層困難な、極めて複雑なスクランブルが行なわれることになる。

【 0 1 0 0 】

図 1 0、図 1 1 は、特定のビットのみスクランブルをかけるためのマスクパターンが付加されたスクランブル演算回路の各例を示す図である。

【 0 1 0 1 】

図 1 0 に示すスクランブル演算回路は、1 つの反転回路と、2 つの論理積回路と、1 つの加算回路とからなり、この回路の場合、

$$\text{OUT} = (\text{IN} \text{ and } \text{M}) + \text{SP} + (\text{IN} \text{ and } (\text{not } \text{M})) \quad \dots (6)$$

の演算が行なわれる。

【 0 1 0 2 】

ここで、M はマスクパターンを表わし、そのマスクパターン M の中の、0 が設定されたビットについては、スクランブルは行なわれない。例えば、1 6 ビットのうち下位 4 ビットのスクランブルを禁止するときは、マスクパターン M として 0 x F F F 0 が設定される。

【 0 1 0 3 】

また、図 1 1 に示すスクランブル演算回路は、1 つの反転回路、2 つの論理積回路、2 つの加算回路、および 1 つの排他的論理和回路が図 1 1 に示すように接続されたものであり、ここでは、

$$\begin{aligned} \text{OUT} = & ((\text{IN} \text{ and } \text{M}) + \text{SP} 1) \text{ XOR } \text{SP} 2) \\ & + (\text{IN} \text{ and } (\text{not } \text{M})) \quad \dots (7) \end{aligned}$$

の演算が行なわれる。

【 0 1 0 4 】

以上例示したように、スクランブル演算回路として様々な演算回路を採用することができる。

【 0 1 0 5 】

図 1 2 は、図 4 に示す第 2 実施形態の処理装置 5 におけるアドレスマップであ

る。

【 0 1 0 6 】

図 4 には、代表的に RAM は 1 つのみ示したが、実際にはワーク RAM とバックアップ RAM を備えており、ワーク RAM には、0 x 0 0 0 0 0 0 ~ 0 x 0 F F F F F のアドレス領域（ワーク RAM 領域）が割り当てられており、バックアップ RAM には、装置の電源が切断された状態であっても電池等によりバックアップされ、その内容が保持されている。

【 0 1 0 7 】

また、0 x 2 0 0 0 0 0 ~ 0 x 2 F F F F F は I O 領域、0 x 3 0 0 0 0 0 ~ 0 x 3 F F F F F はフラッシュ ROM 領域である。フラッシュ ROM には、各種のアプリケーションプログラムが格納されている。図 4 に示すアドレスバススクランブルパターンメモリ 5 0 4 およびデータバススクランブルパターンメモリ 5 0 6 は、I O 領域（0 x 2 X X X X の領域）に割り当てられている。

【 0 1 0 8 】

ここで、図 4 に示すデコーダ回路は、アドレス A 4 ~ 1 9 に基づいて、表 1 の真理値表に従って、データバススクランブルパターンメモリ 5 0 6 のライトイネーブル信号 * W E P M D およびアドレスバススクランブルパターンメモリ 5 0 4 のライトイネーブル信号 * W E P M A を出力する。

【 0 1 0 9 】

【表 1】

A19	A18	A17	A16~5	A4	*WEPMD	*WEPMA
0	0	1	ALL 0	0	0	1
0	0	1	ALL 0	1	1	0
1	*	*	*	*	1	1
*	1	*	*	*	1	1
*	*	0	*	*	1	1
*	*	*	≠ ALL 0	*	1	1

【 0 1 1 0 】

この表 1 は、0 x 2 0 0 0 X のときにデータバススクランブルパターンメモリ 5 0 6 を書込み可能状態（* W E P M D = 0）とし、0 x 2 0 0 1 X のときにア

ドレスバススクランブルパターンメモリ 5 0 4 を書き込み可能状態 (*WE PMA = 0) とすることを意味している。

【0 1 1 1】

図 1 3 は、データバススクランブルパターンメモリ 5 0 6 の構成を示す図である。このデータバススクランブルパターンメモリ 5 0 6 は、2 つのデコーダ（デコーダ 1 とデコーダ 2）と、4 つのデータラッチ（データラッチ 0 ～ 3）で構成されている。データラッチ 0 ～ 3 は、それぞれ、ワーク RAM, バックアップ RAM, I O, フラッシュ ROM のデータをスクランブルするための各スクランブルパターンの格納領域であり、後に示す表 4 にあるように、それぞれ、アドレス 0 x 2 0 0 0, 0 x 2 0 0 1, 0 x 2 0 0 2, 0 x 2 0 0 3 が割り当てられている。

【0 1 1 2】

デコーダ 1 は、各データラッチ 0 ～ 3 に格納されている各スクランブルパターンを選択的に出力させるための各アウトプットイネーブル信号 *OE 0 ～ *OE 3 を生成する回路であり、表 2 の真理値表に示す論理構成となっている。

【0 1 1 3】

【表 2】

A19	A18	A17	A16	*OE0	*OE1	*OE2	*OE3
0	0	0	0	0	1	1	1
0	0	0	1	1	0	1	1
0	0	1	0	1	1	0	1
0	0	1	1	1	1	1	0
1	*	*	*	1	1	1	1
*	1	*	*	1	1	1	1

【0 1 1 4】

また、デコーダ 2 は、各データラッチ 0 ～ 3 に新たなスクランブルパターンを書き込むための各ライトイネーブル信号 *WE 0 ～ *WE 3 を生成する回路であり、表 3 の真理値表に示す論理構成となっている。

【0 1 1 5】

【表 3】

*WEPMD	A0	A1	*WE0	*WE1	*WE2	*WE3
1	*	*	1	1	1	1
0	0	0	0	1	1	1
0	0	1	1	0	1	1
0	1	0	1	1	0	1
0	1	1	1	1	1	0

【0 1 1 6】

データラッチ 0～3 は、各々に対応するライトイネーブル信号 *WE 0～3 が 0 になると、そのタイミングでデータバス 5 1 2 に出力されている D 0～7 のデータを記憶し、また、各々に対応するアウトプットイネーブル信号 *OE 0～3 が 0 になると記憶しているスクランブルパターンを SPD 0～7 のデータとして出力する。ここで、アウトプットイネーブル信号 *OE 0～3 の全てが 1 の場合は、SPD 0～7 のデータは全てのビットが 0 となる。

【0 1 1 7】

ここで、本実施形態では、データバス 5 1 2 上のデータは 8 ビット幅 (D 0～7) であるのに対し、アドレスバス 5 1 1 は、スクランブルとは無関係の拡張ビット SA 1 6～1 9 を除き 1 6 ビット幅 (A 0～A 1 5) である。図 1 3 にはデータバススクランブルパターンメモリ 5 0 6 の構成を示したが、アドレスバススクランブルパターンメモリ 5 0 4 は、データと比べてアドレスのビット幅が広いことに伴い、図 1 3 に示すデータラッチ 0～3 がそれぞれ 2 バイト構成になり、各データラッチを選択するためのアドレスが A 0～3 の 4 ビット (図 1 3 に示すデータバススクランブルパターンメモリ 5 0 6 の場合はデータラッチを選択するためのアドレスは A 0～1 の 2 ビットである) となることを除き、構成としては図 1 3 に示すデータバススクランブルパターンメモリ 5 0 6 の構成と同様であり、アドレスバススクランブルパターンメモリ 5 0 4 の図示及びこれ以上の説明は省略する。

【0 1 1 8】

本実施形態では、データバススクランブルパターンメモリ 5 0 6 の各データラッチ 0～3 およびアドレスバススクランブルパターンメモリ 5 0 4 の各データラ

ッチには、表 4 に示すアドレスが割り当てられており、各アドレスにそれらの各アドレスに対応するスクランブルの各対象領域についてスクランブルを実行するためのスクランブルパターンが書き込まれ、CPU 501 から出力されるアドレス情報（A0～19）に従って、各データラッチに書き込まれているスクランブルパターンがスクランブル演算回路に向けて出力される。

【0119】

【表 4】

アドレス	対象メモリ	対象ラッチ名	対象領域
20000	データバス スクランブル パターン メモリ	データラッチ 0	ワーク RAM
20001		データラッチ 1	バックアップ RAM
20002		データラッチ 2	I/O
20003		データラッチ 3	フラッシュ ROM
20008	アドレスバス スクランブル パターン メモリ	データラッチ 0 下位バイト	ワーク RAM
20009		データラッチ 0 上位バイト	
2000A		データラッチ 1 下位バイト	バックアップ RAM
2000B		データラッチ 1 上位バイト	
2000C		データラッチ 2 下位バイト	I/O
2000D		データラッチ 2 上位バイト	
2000E		データラッチ 3 下位バイト	フラッシュ ROM
2000F		データラッチ 3 上位バイト	

【0120】

表 5 は、本実施形態におけるパターンメモリの設定例を示す表である。

【0121】

【表 5】

領域	アドレス範囲	アドレスバス スクランブルパターン	データバス スクランブルパターン
ワーク RAM	0x00000～ 0x0FFFF	0x3CB0	0x25
バックアップ RAM	0x10000～ 0x1FFFF	0x2A50	0x6E
I/O	0x20000～ 0x2FFFF	0x0000	0x00
フラッシュROM	0x30000～ 0x3FFFF	0x41D9	0x2B

【0122】

本実施形態で採用されている R A M は、下位 4 ビットについて連続したアドレスでアクセスした場合に高速なアクセスが可能な素子であり、したがって表 5 に示すように、R A M のアドレスバススクランブルパターンの下位 4 ビットは 0 (スクランブルを行なわないことを意味する) に設定されており、C P U からの連続したメモリアクセスの場合の高速なアクセス速度を保証している。

【 0 1 2 3 】

また、I O 空間はスクランブルを禁止するために、全てのビットが 0 に設定されている。

【 0 1 2 4 】

図 1 4 は、図 4 に示す処理装置における、電源投入時およびリセット時に動作するプログラムの一部を示した図である。

【 0 1 2 5 】

ここでは、1 6 ビットの乱数 R A と 8 ビットの乱数 R D が生成され (ステップ b 1 , b 2) 、1 6 ビットの乱数 R A と 0 x F F F 0 との論理積演算結果がアドレス 0 x 2 0 0 0 8 ~ 9 に書き込まれ (ステップ b 3) 、8 ビットの乱数 R D がアドレス 0 x 2 0 0 0 0 に書き込まれる。表 4 に示すようにアドレス 0 x 2 0 0 0 8 ~ 9 はワーク R A M 用のアドレスバススクランブルパターンの格納領域、アドレス 0 x 2 0 0 0 0 はワーク R A M 用のデータバススクランブルパターンの格納領域である。

【 0 1 2 6 】

すなわち、ここでは、電源投入あるいはリセットのたびにワーク R A M のスクランブルパターンが変更されることになり、このことも、外部からの不正な解析を一層困難にするのに役立っている。

【 0 1 2 7 】

尚、バックアップ R A M やフラッシュ R O M については、そこに格納されたデータやプログラムの一貫性が必要なため、あらかじめ定められたスクランブルパターンがそのまま保持され、電源の再投入やリセットが行なわれても、スクランブルパターンは変更されない。

【 0 1 2 8 】

フラッシュROMについては、工場での書込み時にはスクランブルをかけないでおくことも可能である。その場合、出荷後の最初の電源投入時に、以下の手順によりスクランブルがかけられる。

【0129】

図15は、電源投入時に動作するプログラムの、フラッシュROMのスクランブルの部分を示すフローチャートである。

【0130】

ここでは、まず、フラッシュROMの内容がスクランブルされたものであるか否かを示すスクランブル有無フラグがチェックされる。このスクランブル有無フラグはバックアップRAMの所定の番地に格納されており、工場での書込み時に、このスクランブル有無フラグは‘無’に設定される。

【0131】

このスクランブル有無フラグの確認は、フラッシュROMの内容が既にスクランブル済であるか否かの判定のためであり、スクランブル有無フラグを設定する代わりに、フラッシュROMに対応するスクランブルパターンを読み出し、そのスクランブルパターンの全ビットが0であることをもって、未だスクランブルが行なわれていないものと判定してもよい。

【0132】

ステップc1でスクランブル有無フラグがスクランブル‘無’に設定されていると判定されると、ステップc2に進み、フラッシュROMの内容がRAMにコピーされる。このフラッシュROMの一部には、以下の処理を行なうためのプログラムが書込まれている。

【0133】

次いで、RAMにコピーされたプログラムのうち、以下の処理を行なうためのプログラムに制御が移され、フラッシュROMが消去され（ステップc4）、16ビットの乱数RAと8ビットの乱数RDが生成され（ステップc5、c6）、16ビットの乱数RAがフラッシュROMのアドレススクランブルパターンとしてアドレス0x2000E～Fに書き込まれるとともに8ビットの乱数RDがフラッシュROMのデータスクランブルパターンとしてアドレス0x20003に

書き込まれる（表 4 を参照；ステップ c 7， c 8）。

【 0 1 3 4 】

次に、ステップ c 2 で RAM にコピーされたプログラムが、アドレス 0 x 2 0 0 0 E ~ F およびアドレス 0 x 2 0 0 0 3 に書き込まれたアドレススクランブルパターンおよびデータスクランブルパターンでスクランブルされてフラッシュ ROM に書き戻され（ステップ c 9）、フラッシュ ROM スクランブル有無フラグが‘有’に変更される（ステップ c 1 0）。

【 0 1 3 5 】

こうすることにより、フラッシュ ROM の内容が最初の電源投入時にスクランブルされることになる。

【 0 1 3 6 】

また、工場出荷時には特定のスクランブルパターンでスクランブルしておいて、最初の電源投入時に別のスクランブルパターンでスクランブルし直すようにしてもよい。この場合、工場出荷時にスクランブルされた内容を元に戻すための逆スクランブルパターン（ここではスクランブルパターンを参照することによって元に戻すことができるためスクランブルパターンそのものである）は、スクランブルパターンメモリに書き込んでおくこともでき、フラッシュ ROM 内に書き込んでおいてもよい。フラッシュ ROM 内に書き込んでおくと、工場出荷時点ではスクランブルパターンメモリについて電池等でバックアップしておく必要がないという利点がある。

【 0 1 3 7 】

図 1 6 は、フラッシュ ROM に、あらかじめスクランブルされたプログラムが書き込まれており、かつそのスクランブルを元に戻すのに必要なスクランブルパターンがフラッシュ ROM 内に格納されて出荷されたときの、電源投入時に動作するプログラムの、フラッシュ ROM のスクランブルの部分を示すフローチャートである。このプログラムは、図 1 5 に示すプログラムに代えて実行されるプログラムである。

【 0 1 3 8 】

ステップ d 1 では、工場出荷前のスクランブルを除き、フラッシュ ROM が既

にスクランブルされたか否かを示すスクランブル有無フラグが参照される。工場出荷前のスクランブルを除き、未だ一度もスクランブルされていないときはステップ d 2 ～ d 1 2 の各ステップが実行される。

【 0 1 3 9 】

ステップ d 2, d 3 では、フラッシュ ROM に格納されている、アドレスバススクランブルパターン S P A 0 およびデータバススクランブルパターン S P D 0 がそれぞれアドレス 0 x 2 0 0 0 E ～ F およびアドレス 0 x 2 0 0 0 3 に書き込まれる（表 4 参照）。

【 0 1 4 0 】

次にステップ d 4 において、フラッシュ ROM の内容がスクランブルパターン S P A 0, S P D 0 に基づいてスクランブルされる前の状態に戻されて RAM にコピーされる。

【 0 1 4 1 】

その後の各ステップ d 5 ～ d 1 2 は、図 1 5 の各ステップ c 3 ～ c 1 0 とそれぞれ同一であり、重複説明は省略する。

【 0 1 4 2 】

この図 1 6 に示すプログラムの実行により、フラッシュ ROM の内容が、最初の電源投入時に新たに生成した乱数 R A, R B をアドレススクランブルパターン, データスクランブルパターンとして再度スクランブルされ、その後はそのスクランブルされた状態が保持される。

【 0 1 4 3 】

ここで、上記の例は、スクランブルパターンがフラッシュ ROM に書き込まれた例であるが、例えばフラッシュ ROM の内容を、工場出荷前に、個々の製品毎に別々のスクランブルパターンでスクランブルしておき、そのスクランブルを解除するための逆スクランブルパターンを特定の暗号処理により暗号化して、バックアップ RAM 等、フラッシュ ROM とは別の領域に書き込んでおいてもよい。そのときはその暗号化されたスクランブルパターンを暗号化前のスクランブルパターンに戻すための復号処理の手続も、L S I 5 0 の内部のいずれかの領域に埋め込まれる。

【0144】

上記の暗号処理としては、例えば公開鍵暗号方式（例えばR A S等）を用いることができる。すなわち、公開鍵（K p b）で暗号化された逆スクランブルパターンをフラッシュROMあるいは他のメモリに書き込んでおき、その暗号化されたスクランブルパターンをL S I 5 0内のいずれかの領域に埋め込んでおいた秘密鍵（K p v）で復号する。このようなシステムの場合、同一仕様のL S I 5 0を複数の会社で使用した場合であっても、各会社に公開鍵のみを渡し、秘密鍵は伏せておくことにより、会社間のセキュリティが確保できる。

【0145】

図17は、フラッシュROMについて工場出荷前にスクランブルしておき、そのスクランブルを解除するためのスクランブルパターンを公開鍵K p bにより暗号化してバックアップRAMに格納し、その状態で出荷された後の電源投入時に動作するプログラムの、フラッシュROMのスクランブルの部分を示すフローチャートである。

【0146】

ステップe 2, e 3では、バックアップRAMより、公開鍵で暗号化された状態のアドレスバススクランブルパターンK p b（S P A 0）が読み出され、L S Iの内部に埋め込まれた秘密鍵K p vにより復号化されて平文のアドレスバススクランブルパターンS P A 0が取り出される。

【0147】

また、ステップe 4, e 5では、バックアップRAMより、公開鍵で暗号化された状態のデータバススクランブルパターンK p b（S P D 0）が読み出され、L S Iの内部に埋め込まれた秘密鍵K p vにより復号化されて平文のデータバススクランブルパターンが取り出される。

【0148】

ステップe 6, e 7では、上記のようにして得られた平文のアドレスバススクランブルパターンS P A 0および平文のデータバススクランブルパターンS P D 0が、それぞれ、アドレス0 x 2 0 0 0 E ~ Fおよびアドレス0 x 2 0 0 0 3に書き込まれる（表4参照）。

【0149】

その後の各ステップ e 8 ～ e 1 6 は、図 1 6 の各ステップ d 4 ～ d 1 2 とそれぞれ同一であり、重複説明は省略する。

【0150】

図 1 8 は、本発明の処理装置の第 3 実施形態のブロック図である。

【0151】

図 4 に示す第 2 実施形態からの相違点について説明する。

【0152】

この第 3 実施形態では、外部回路 6 0 0 に、図 4 の第 2 実施形態と同様の R A M 6 0 1 およびフラッシュ R O M 6 0 2 が備えられているほか、さらに通信制御回路 6 0 3 が備えられている。

【0153】

この通信制御回路 6 0 3 は通信回路網 8 0 0 を介して鍵管理センター 7 0 0 と接続されている。フラッシュ R O M 6 0 2 には、工場出荷前にスクランブルされた状態のプログラムが格納されており、最初の電源投入時に、鍵管理センター 7 0 0 から、通信回路網 8 0 0 を経由して、暗復号化されたスクランブルパターンを受け取るように構成されている。

【0154】

図 1 9 は、図 1 8 に示す処理装置における電源投入時に実行されるプログラムの、フラッシュ R O M のスクランブルに関する部分のフローチャートである。

【0155】

図 1 9 のステップ f 1 は、図 1 7 のステップ e 1 と同じである。

【0156】

ステップ f 2 では鍵管理センターへの接続が行なわれ、ステップ f 3 では、鍵管理センターから、公開鍵 K p b で暗号化された形式のアドレスバススクランブルパターン k p b (S P A 0) およびデータバススクランブルパターン K p b (S P D 0) がダウンロードされる。

【0157】

ステップ f 4 , f 5 では、L S I に埋め込まれた秘密鍵 K p v により、暗号化

された状態のアドレスバススクランブルパターン $Kpb(SPA0)$ および暗号化された状態のデータバススクランブルパターン $Kpb(SPDO)$ がそれぞれ復号化されて、平文のアドレスバススクランブルパターン $SPA0$ およびデータバススクランブルパターン $SPDO$ が取り出される。

【0158】

それ以降の各ステップ $f6 \sim f16$ は図17の各ステップ $e6 \sim e16$ とそれぞれ同一であり、重複説明は省略する。

【0159】

このように、通信により鍵管理センター等の外部からスクランブルパターンの入手を可能とすることにより、システムの柔軟性が確保される。

【0160】

図20は、本発明の処理装置の第4実施形態のブロック図である。

【0161】

図4に示す第2実施形態との相違点について説明する。

【0162】

図20に示す第4実施形態では、外部回路600に、図4の第2実施形態の場合と同様のRAM601およびラッシュROM602が備えられているほか、タンパ検出スイッチ604が備えられており、さらにバックアップ用電池605が明示的に示されている。

【0163】

アドレスバススクランブルパターンメモリ504およびデータバススクランブルパターンメモリ506は、電源が切断された状態においてもバックアップ用電池605からの電力によりその内容が消去されないようバックアップされている。

【0164】

ここで、この処理装置5が不正に開けられた場合にタンパ検出スイッチ604が働き、バックアップ用電池605からの電力供給経路が遮断され、アドレスバススクランブルパターンメモリ504およびデータバススクランブルパターンメモリ506に格納されていたアドレスバススクランブルパターンおよびデータバ

ススクランブルパターンが消去され、この処理装置の動作が不能となる。こうすることにより、不正な解析がさらに確実に防止される。

【 0 1 6 5 】

尚、上記の各実施形態では、1つのLSIの内部に作り込まれた回路を内部回路、そのLSIの外部に外付けされたデバイスの集合を外部回路と称しているが、内部回路は必ずしも1つのLSIに搭載されたものである必要はなく、例えば複数のLSIに分散して搭載されてそれら複数のLSIが1つの集積回路パッケージ内にパッケージされ、あるいは、それら複数のLSIが一体にモールドされたものである場合に、それら複数のLSIに分散して搭載された回路全体を内部回路と称してもよい。

【 0 1 6 6 】

以下、本発明の各種態様を付記する。

【 0 1 6 7 】

(付記1) プログラムを実行するCPUと、各所定の作用を成す1つ以上の内部デバイスと、前記CPUと前記内部デバイスとを結ぶとともに外部にまで延びアドレスおよびデータを伝達するバスラインとを含む内部回路、および

前記バスラインの外部に延びた部分に外付けされた、各所定の作用を成す1つ以上の外部デバイスを含む外部回路を備え、

前記内部回路が、前記バスラインの、外部への出入口に介在し、該バスライン上のアドレスおよびデータを、前記1つ以上の外部デバイス全体に割り当てられたアドレス空間を複数に分けた各領域に応じた各暗号化パターンで暗号化する暗号化部を含むものであることを特徴とする処理装置。

【 0 1 6 8 】

(付記2) 前記暗号化部で採用される暗号化パターンには、アドレスおよびデータの双方とも暗号化しないことを1つの暗号化パターンとして含むものであることを特徴とする付記1記載の処理装置。

【 0 1 6 9 】

(付記3) 前記外部回路が複数の外部デバイスを含むものであり、前記暗号化部は、前記複数の外部デバイスそれぞれに応じた暗号化パターンで

暗号化するものであることを特徴とする付記 1 記載の処理装置。

【0170】

(付記 4) 前記暗号化部は、前記外部回路がアクセスされていないタイミングで、前記バスラインの、外部に延びた部分に、ダミーのアドレスおよびデータを出力するものであることを特徴とする付記 1 記載の処理装置。

【0171】

(付記 5) 前記 CPU は、クロックの供給を受け供給されたクロックに同期してプログラムを実行するものであるとともに、前記暗号化部も、クロックの供給を受け供給されたクロックに同期して暗号化を行なうものであって、

前記暗号化部に、前記 CPU に供給されるクロックよりも高速なクロックを供給するクロック供給部を備えたことを特徴とする付記 1 記載の処理装置。

【0172】

(付記 6) 前記外部回路の構成を認識し、その構成に応じて、前記暗号化部における暗号化パターンを決定する暗号化パターン決定手段を有することを特徴とする付記 1 記載の処理装置。

【0173】

(付記 7) 前記暗号化部は、前記バスライン上のアドレスおよびデータを、前記 1 つ以上の外部デバイス全体に割り当てられたアドレス空間を複数に分けた各領域に応じるとともに前記 CPU で実行されるアプリケーションプログラムにも応じた暗号化パターンで暗号化するものであることを特徴とする付記 1 記載の処理装置。

【0174】

(付記 8) 前記バスラインの、外部に延びた部分に接続され、該バスライン上の暗号化されたアドレスおよびデータを暗号化前のアドレスおよびデータに戻す逆暗号化部を備えたことを特徴とする付記 1 記載の処理装置。

【0175】

(付記 9) 前記 1 つ以上の外部デバイス全体に割り当てられたアドレス空間を複数に分けた複数の領域のうちのいずれかの領域について、所定の初期化動作の都度暗号化パターンを変更する暗号化パターン変更手段を有することを特徴

とする付記 1 記載の処理装置。

【 0 1 7 6 】

(付記 1 0) 前記暗号化部は、前記 1 つ以上の外部デバイス全体に割り当てられたアドレス空間を複数に分けた複数の領域のうちのいずれかの領域について、暗号化後のデータがアドレスに応じて変化する暗号化パターンを採用して、データを暗号化するものであることを特徴とする付記 1 記載の処理装置。

【 0 1 7 7 】

(付記 1 1) プログラムを実行する CPU と、各所定の作用を成す 1 つ以上の内部デバイスと、前記 CPU と前記内部デバイスとを結ぶとともに外部にまで延びアドレスおよびデータを伝達するバスラインとを含む内部回路、および

前記バスラインの、外部に延びた部分に外付けされた、情報を記憶するメモリを含む外部回路を備え、

前記内部回路が、前記メモリに記憶された情報のうちの少なくとも一部の情報を、所定の初期化動作で暗号化して書き換える情報書換手段を有するものであることを特徴とする処理装置。

【 0 1 7 8 】

(付記 1 2) 前記所定の初期化動作が、最初の電源投入時の初期化動作であることを特徴とする付記 1 記載の処理装置。

【 0 1 7 9 】

(付記 1 3) 前記情報書換手段は、乱数を発生させ、発生させた乱数を用いた暗号化パターンを採用して暗号化を行なうものであることを特徴とする付記 1 1 記載の処理装置。

【 0 1 8 0 】

(付記 1 4) 前記メモリに記憶された情報のうちの少なくとも一部の情報が、前記所定の初期化動作を実行する以前において既に暗号化されたものであって、

前記情報書換手段は、該少なくとも一部の情報を一旦暗号化前の情報に戻し異なる暗号化パターンを採用して再度暗号化を行なって書き換えるものであることを特徴とする付記 1 1 記載の処理装置。

【 0 1 8 1 】

(付記 1 5) 前記少なくとも一部の情報を暗号化前の情報に戻すための復号化情報が前記メモリに記憶されてなるものであって、

前記情報書換手段は、該少なくとも一部の情報を、該復号化情報を用いて一旦暗号化前の情報に戻すものであることを特徴とする付記 1 4 記載の処理装置。

【 0 1 8 2 】

(付記 1 6) 前記少なくとも一部の情報が公開鍵により暗号化されたものであるとともに、この処理装置は秘密鍵が埋め込まれてなるものであって、

前記情報書換手段は、該少なくとも一部の情報を該秘密鍵を用いて一旦暗号化前の情報に戻すものであることを特徴とする付記 1 4 記載の処理装置。

【 0 1 8 3 】

(付記 1 7) 前記少なくとも一部の情報を暗号化前の情報に戻すための、暗号化された形式の復号化情報を外部より取得する情報取得部を備え、

前記情報書換手段は、前記情報取得部で取得された、暗号化された形式の復号化情報を復号化して平文の復号化情報を取り出しこの平文の復号化情報を用いて該少なくとも一部の情報を一旦暗号化前の情報に戻すものであることを特徴とする付記 1 4 記載の処理装置。

【 0 1 8 4 】

(付記 1 8) 前記内部回路が前記暗号化部で採用される暗号化パターンを保持してなるものであって、

タンパ検出を行なうタンパ検出部を備えるとともに、

前記タンパ検出部によるタンパ検出を受けて前記内部回路内に保持されていた暗号化パターンを破壊する情報破壊手段を備えたことを特徴とする付記 1 又は 1 1 記載の処理装置。

【 0 1 8 5 】

(付記 1 9) プログラムを実行する CPU と、各所定の作用を成す 1 つ以上の内部デバイスと、前記 CPU と前記内部デバイスとを結ぶとともに外部にまで延びて、外部に延びた部分に、各所定の作用を成す 1 つ以上の外部デバイスが外付けされる、アドレスおよびデータを伝達するバスラインと、該バスラインの

、外部への出入口に介在し、該バスライン上のアドレスおよびデータを、該バスラインの、外部に延びた部分に外付けされた1つ以上の外部デバイス全体に割り当てられた空間を複数に分けた各領域に応じた各暗号化パターンで暗号化する暗号化部とが搭載されてなることを特徴とする集積回路。

【0186】

(付記20) 前記暗号化部で採用される暗号化パターンには、アドレスおよびデータの双方とも暗号化しないことを1つの暗号化パターンとして含むものであることを特徴とする付記18記載の集積回路。

【0187】

(付記21) 前記バスラインの、外部に延びた部分に、複数の外部デバイスが外付けされた場合に、前記暗号化部は、前記複数の外部デバイスそれぞれに応じた暗号化パターンで暗号化するものであることを特徴とする付記19記載の集積回路。

【0188】

(付記22) 前記暗号化部は、前記外部回路がアクセスされていないタイミングで、前記バスラインの、外部に延びた部分に、ダミーのアドレスおよびデータを出力するものであることを特徴とする付記19記載の集積回路。

【0189】

(付記23) 前記CPUは、クロックの供給を受け供給されたクロックに同期してプログラムを実行するものであるとともに、前記暗号化部も、クロックの供給を受け供給されたクロックに同期して暗号化を行なうものであって、

前記暗号化部は、前記CPUが動作するクロックよりも高速なクロックで動作するものであることを特徴とする付記19記載の集積回路。

【0190】

(付記24) 前記外部回路の構成を認識し、その構成に応じて、前記暗号化部における暗号化パターンを決定する暗号化パターン決定手段を有することを特徴とする付記19記載の集積回路。

【0191】

(付記25) 前記暗号化部は、前記バスラインの、アドレスおよびデータ

を前記 1 つ以上の外部デバイス全体に割り当てられたアドレス空間を複数に分けた各領域に応じるとともに前記 CPU で実行されるアプリケーションプログラムにも応じた暗号化パターンで暗号化するものであることを特徴とする付記 1 9 記載の集積回路。

【 0 1 9 2 】

(付記 2 6) 前記 1 つ以上の外部デバイス全体に割り当てられたアドレス空間を複数に分けた複数の領域のうちのいずれかの領域について、所定の初期化動作の都度暗号化パターンを変更する暗号化パターン変更手段を有することを特徴とする付記 1 9 記載の集積回路。

【 0 1 9 3 】

(付記 2 7) 前記暗号化部は、前記 1 つ以上の外部デバイス全体に割り当てられたアドレス空間を複数に分けた複数の領域のうちのいずれかの領域について、暗号化後のデータがアドレスに応じて変化する暗号化パターンを採用して、データを暗号化するものであることを特徴とする付記 1 9 記載の集積回路。

【 0 1 9 4 】

(付記 2 8) プログラムを実行する CPU と、各所定の作用を成す 1 つ以上の内部デバイスと、前記 CPU と前記内部デバイスとを結ぶとともに外部にまで延びて、外部に延びた部分に、情報を記憶するメモリが外付けされる、アドレスおよびデータを伝達するバスラインとを備えるとともに、

前記メモリに記憶された情報のうちの少なくとも一部の情報を、所定の初期化動作で暗号化して書き換える情報書換手段を有するものであることを特徴とする集積回路。

【 0 1 9 5 】

(付記 2 9) 前記所定の初期化動作が、最初の電源投入時の初期化動作であることを特徴とする付記 2 8 記載の集積回路。

【 0 1 9 6 】

(付記 3 0) 前記情報書換手段は、乱数を発生させ、発生させた乱数を用いた暗号化パターンを採用して暗号化を行なうものであることを特徴とする付記 2 8 記載の集積回路。

【0197】

(付記31) 前記メモリに記憶された情報のうちの少なくとも一部の情報が、前記所定の初期化動作を実行する以前において既に暗号化されたものであって、

前記情報書換手段は、該少なくとも一部の情報を一旦暗号化前の情報に戻し異なる暗号化パターンを採用して再度暗号化を行なって書き換えるものであることを特徴とする付記28記載の集積回路。

【0198】

(付記32) 前記少なくとも一部の情報を暗号化前の情報に戻すための復号化情報が前記メモリに記憶されてなるものであって、

前記情報書換手段は、該少なくとも一部の情報を、該復号化情報を用いて一旦暗号化前の情報に戻すものであることを特徴とする付記31記載の集積回路。

【0199】

(付記33) 前記少なくとも一部の情報が公開鍵により暗号化されたものであるとともに、この集積回路は秘密鍵が埋め込まれてなるものであって、

前記情報書換手段は、該少なくとも一部の情報を該秘密鍵を用いて一旦暗号化前の情報に戻すものであることを特徴とする付記31記載の集積回路。

【0200】

(付記34) 前記少なくとも一部の情報を暗号化前の情報に戻すための、暗号化された形式の暗号化情報を外部より取得する情報取得部を備え、

前記情報書換手段は、前記情報取得部で取得された、暗号化された形式の復号化情報を復号化して平文の復号化情報を取り出しこの平文の復号化情報を用いて該少なくとも一部の情報を一旦暗号化前の情報に戻すものであることを特徴とする付記31記載の集積回路。

【0201】

【発明の効果】

以上、説明したように、本発明によれば、外付けされたデバイスにプログラムやデータ等を記憶させても、それらを第3者による不正なりバースエンジニアリング等の行為から守る事ができ、従来よりも高いセキュリティを保つことができ

る。

【図面の簡単な説明】

【図 1】

本発明の処理装置の第 1 実施形態を示すブロック図である。

【図 2】

図 1 に示す処理装置のメモリマップを示す図である。

【図 3】

図 1 に示す処理装置に電源が投入されたときに実行される初期化プログラムのフローチャートである。

【図 4】

本発明の処理装置の第 2 実施形態のブロック図である。

【図 5】

排他的論理和回路を示す図である。

【図 6】

スクランブル演算回路として採用することのできる回路構成を示した図である。

【図 7】

スクランブル演算回路として採用することのできる回路構成を示した図である。

【図 8】

スクランブル演算回路として採用することのできる回路構成を示した図である。

【図 9】

スクランブル演算回路として採用することのできる回路構成を示した図である。

【図 1 0】

特定のビットのみスクランブルをかけるためのマスクパターンが付加されたスクランブル演算回路の一例を示す図である。

【図 1 1】

特定のビットのみスクランブルをかけるためのマスクパターンが付加されたスクランブル演算回路のもう 1 つの例を示す図である。

【図 1 2】

図 4 に示す第 2 実施形態の処理装置におけるアドレスマップである。

【図 1 3】

データバススクランブルパターンメモリの構成を示す図である。

【図 1 4】

図 4 に示す処理装置における、電源投入時およびリセット時に動作するプログラムの一部を示した図である。

【図 1 5】

電源投入時に動作するプログラムの、フラッシュROMのスクランブルの部分を示すフローチャートである。

【図 1 6】

フラッシュROMにあらかじめスクランブルされたプログラムが書き込まれており、かつそのスクランブルを元に戻すのに必要な逆スクランブルパターンがフラッシュROM内に格納されて出荷されたときの、電源投入時に動作するプログラムの、フラッシュROMのスクランブルの部分を示すフローチャートである。

【図 1 7】

フラッシュROMについて工場出荷前にスクランブルしておき、そのスクランブルを解除するための逆スクランブルパターンを公開鍵K_pbにより暗号化してバックアップRAMに格納し、その状態で出荷された後の電源投入時に動作するプログラムの、フラッシュROMのスクランブルの部分を示すフローチャートである。

【図 1 8】

本発明の処理装置の第 3 実施形態のブロック図である。

【図 1 9】

図 1 8 に示す処理装置における電源投入時に実行されるプログラムの、フラッシュROMのスクランブルに関する部分のフローチャートである。

【図 2 0】

本発明の処理装置の第 4 実施形態のブロック図である。

【符号の説明】

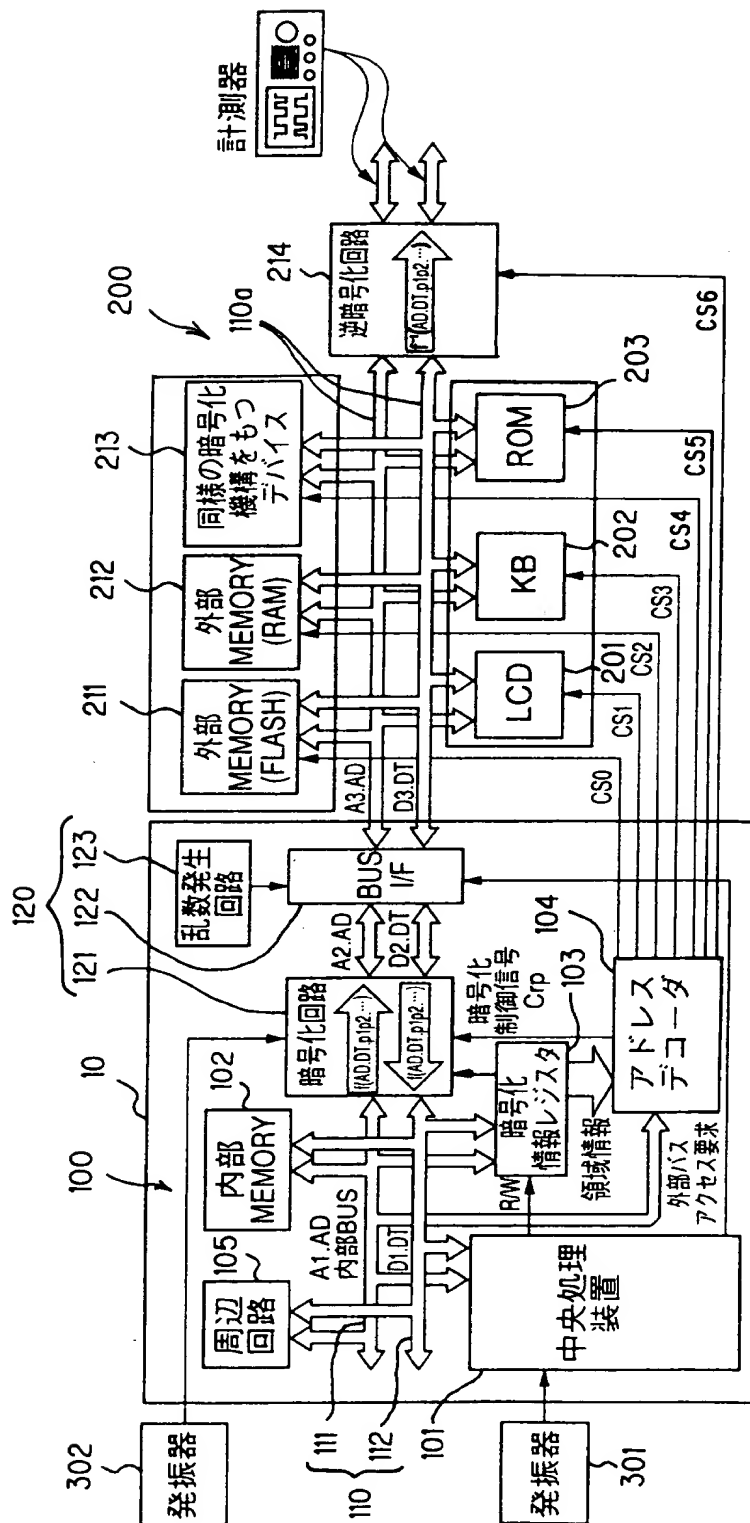
- 1, 5 処理装置
- 1 0, 5 0 L S I
- 1 0 0 内部回路
- 1 0 1 中央処理装置 (C P U)
- 1 0 2 内部メモリ
- 1 0 3 暗号化情報レジスタ
- 1 0 4 アドレスデコーダ
- 1 0 5 周辺回路
- 1 2 0 暗号化部
- 1 2 1 暗号化回路
- 1 2 2 バスインターフェース
- 1 2 3 乱数発生回路
- 2 0 0 外部回路
- 2 0 1 液晶表示装置 (L C D)
- 2 0 2 キーボード (K B)
- 2 0 3 読出専用メモリ (R O M)
- 2 1 1 フラッシュ R O M
- 2 1 2 ランダムアクセスメモリ (R A M)
- 2 1 3 デバイス
- 2 1 4 逆暗号化回路
- 3 0 1, 3 0 2 発振器
- 5 0 0 内部回路
- 5 0 1 C P U
- 5 0 2 内部メモリ
- 5 0 3 アドレスバススクランブル演算回路
- 5 0 4 アドレスバススクランブルパターンメモリ
- 5 0 5 データバススクランブル演算回路

5 0 6	データバススクランブルパターンメモリ
5 0 7	デコード回路
5 1 0	バスライン
5 1 1	アドレスバス
5 1 2	データバス
6 0 0	外部回路
6 0 1	R A M
6 0 2	フラッシュ R O M
6 0 3	通信制御回路
6 0 4	タンパ検出スイッチ
6 0 5	バックアップ用電池
7 0 0	鍵管理センター
8 0 0	通信回路網

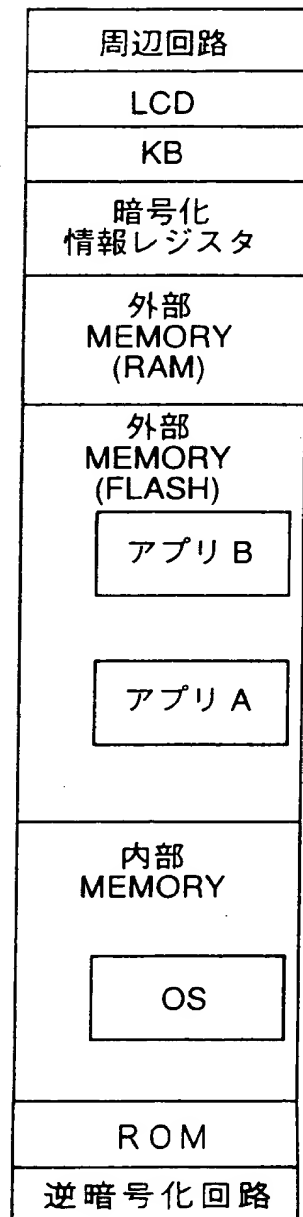
【書類名】

図面

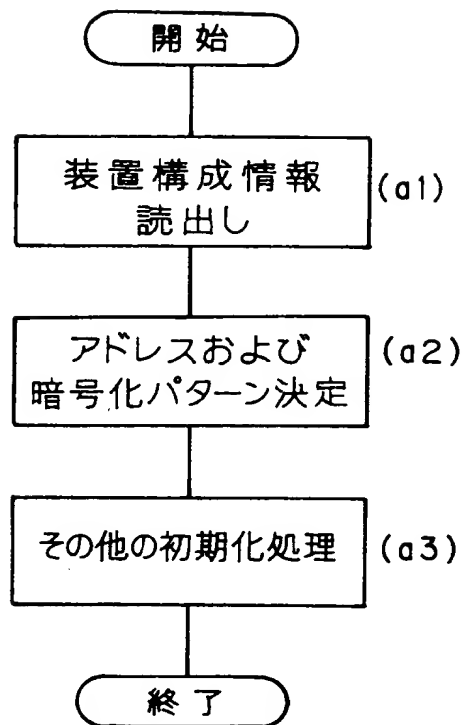
【図 1】



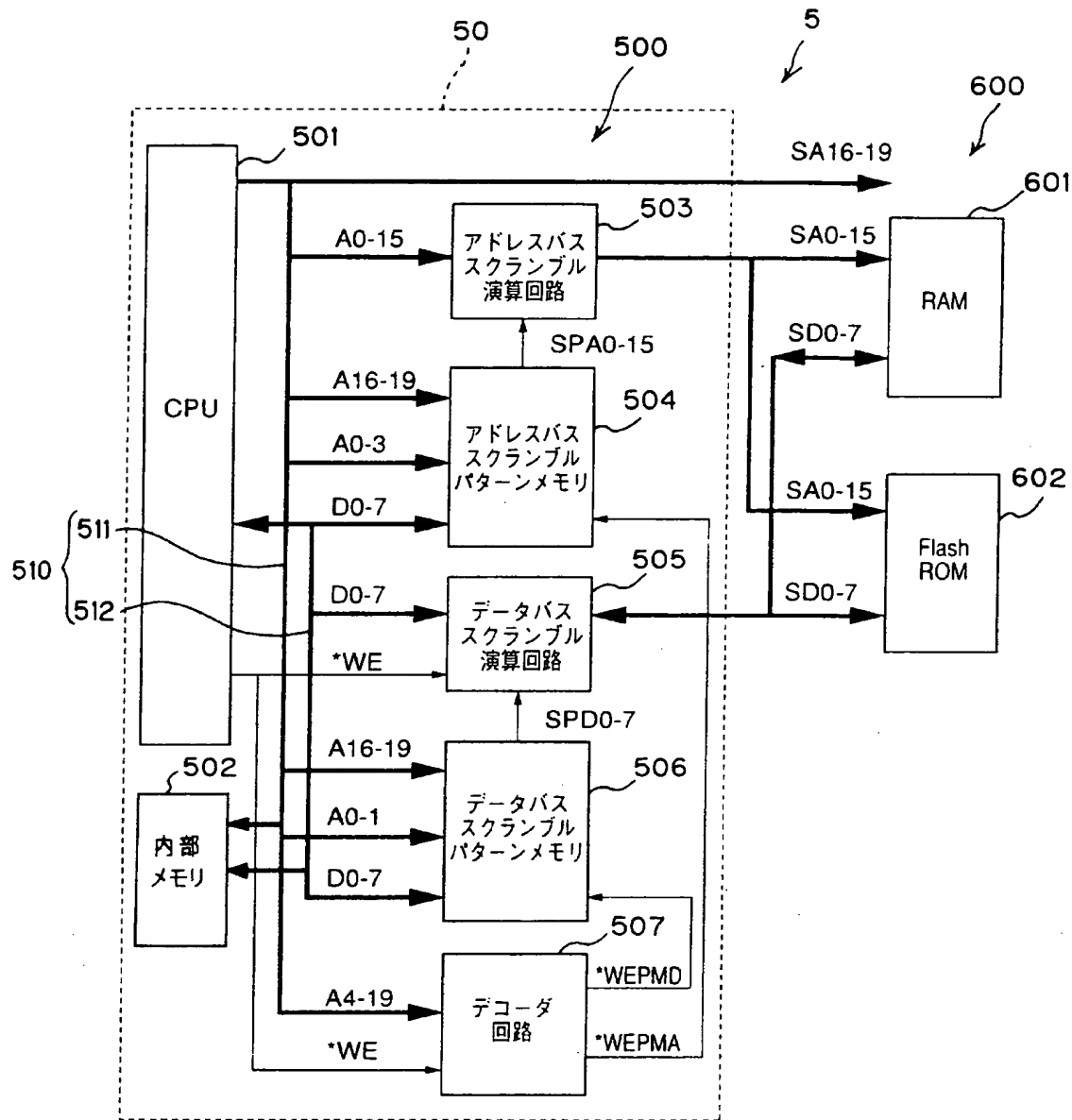
【図 2】



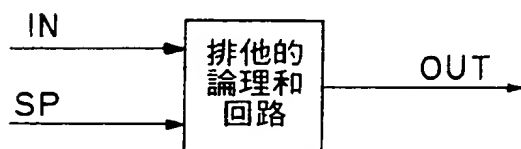
【図 3】



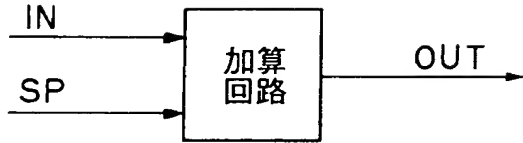
【図 4】



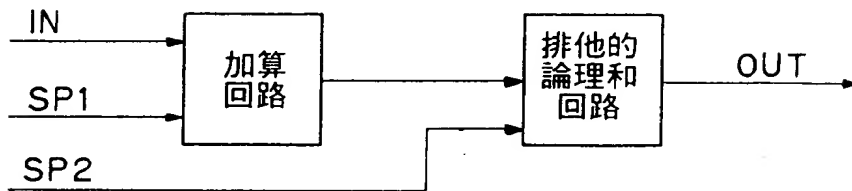
【図 5】



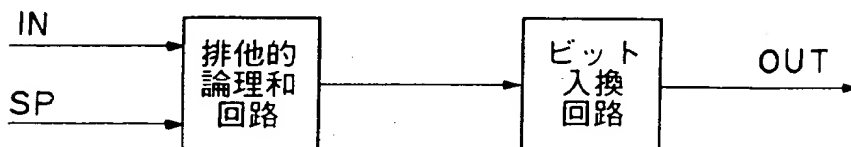
【図 6】



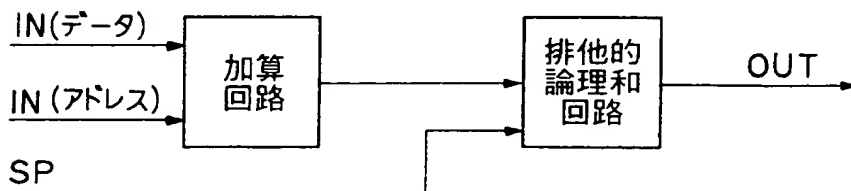
【図 7】



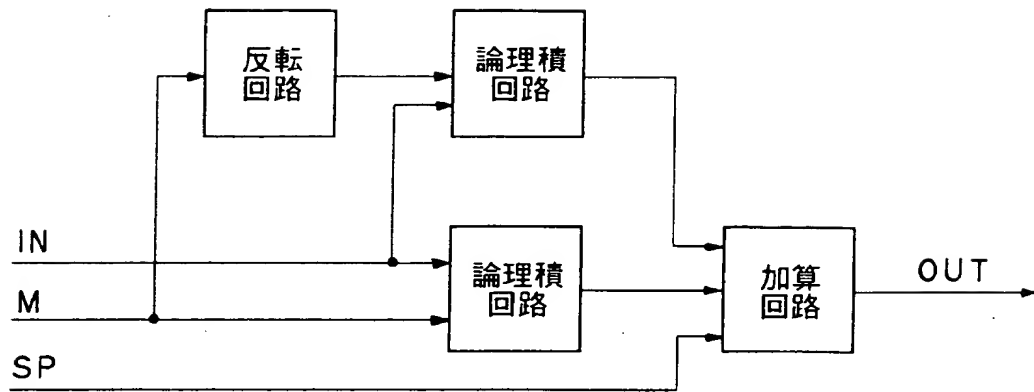
【図 8】



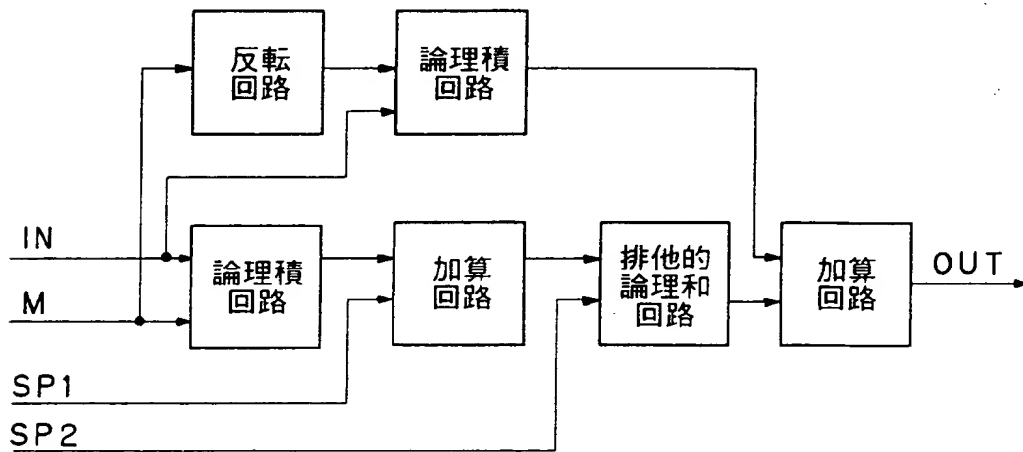
【図 9】



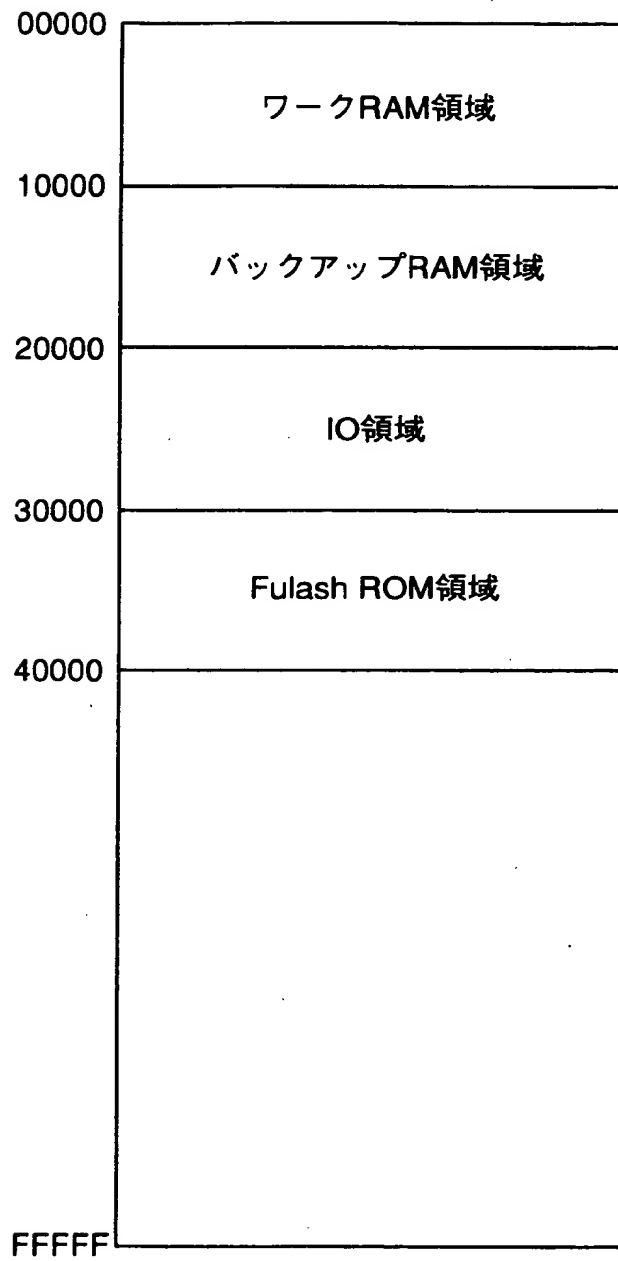
【図 1 0】



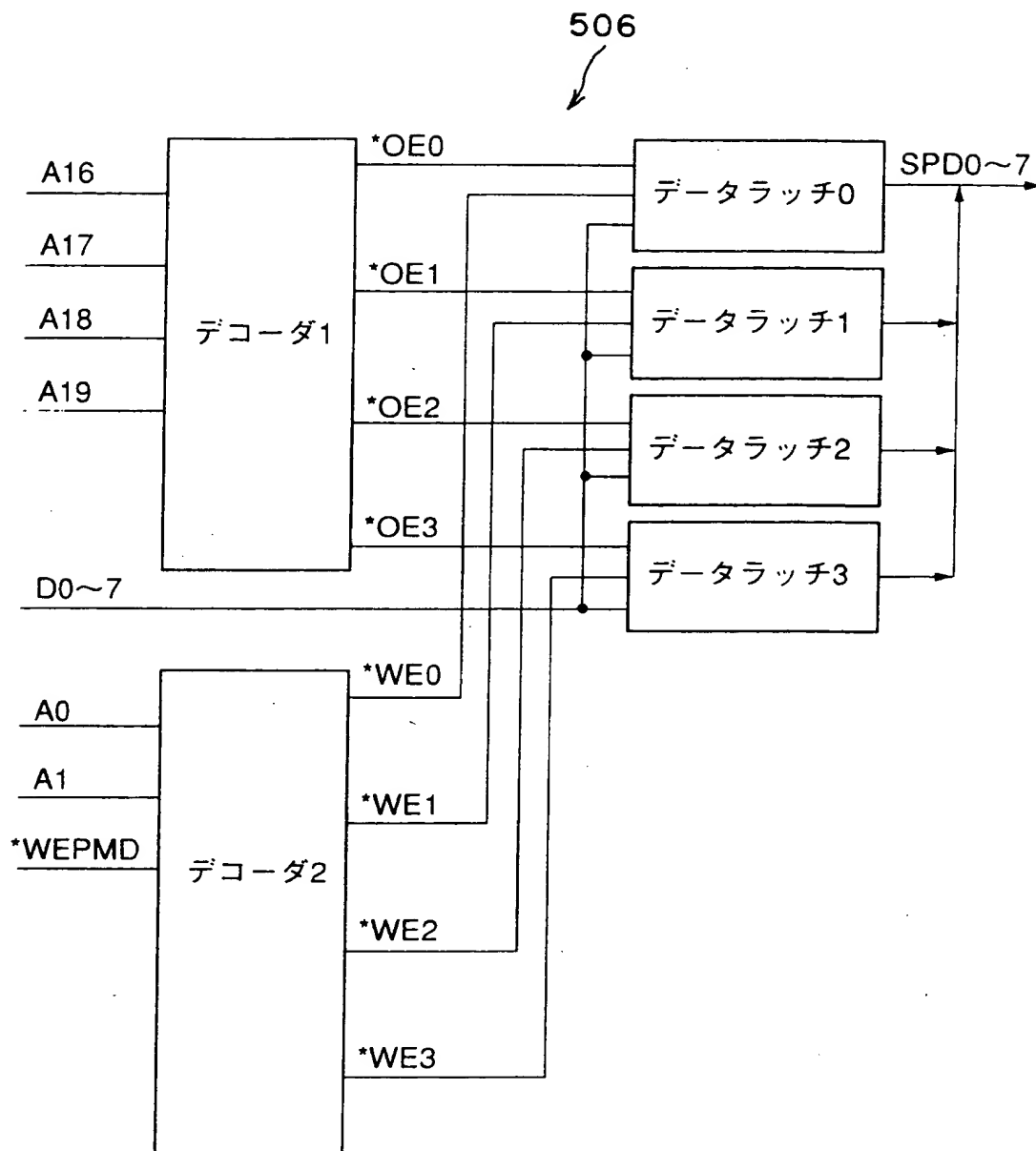
【図 1 1】



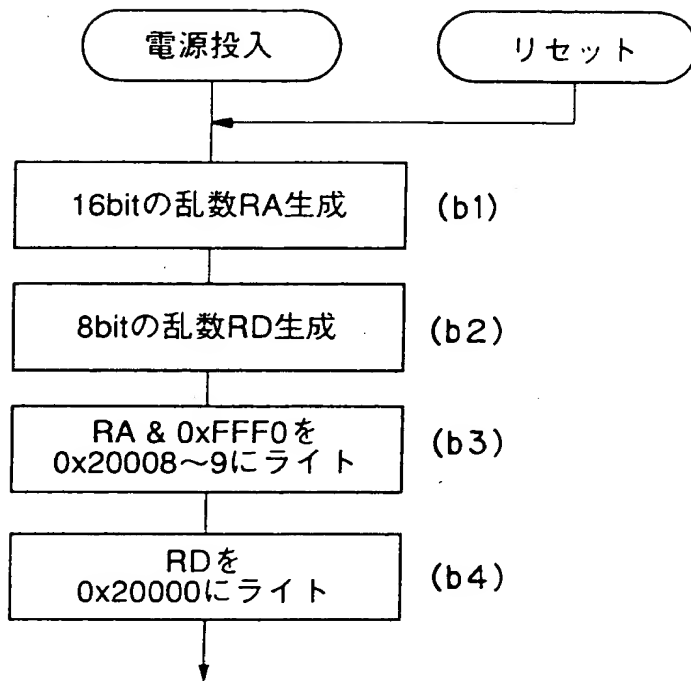
【図 1 2】



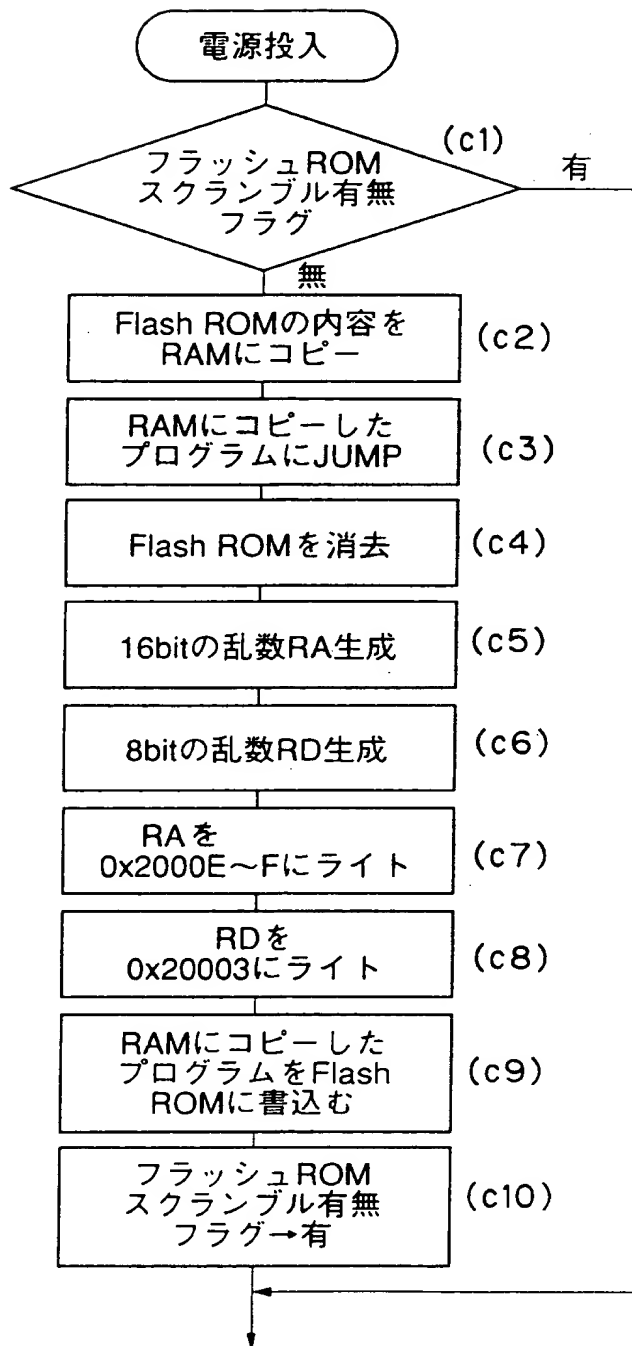
【図 1 3】



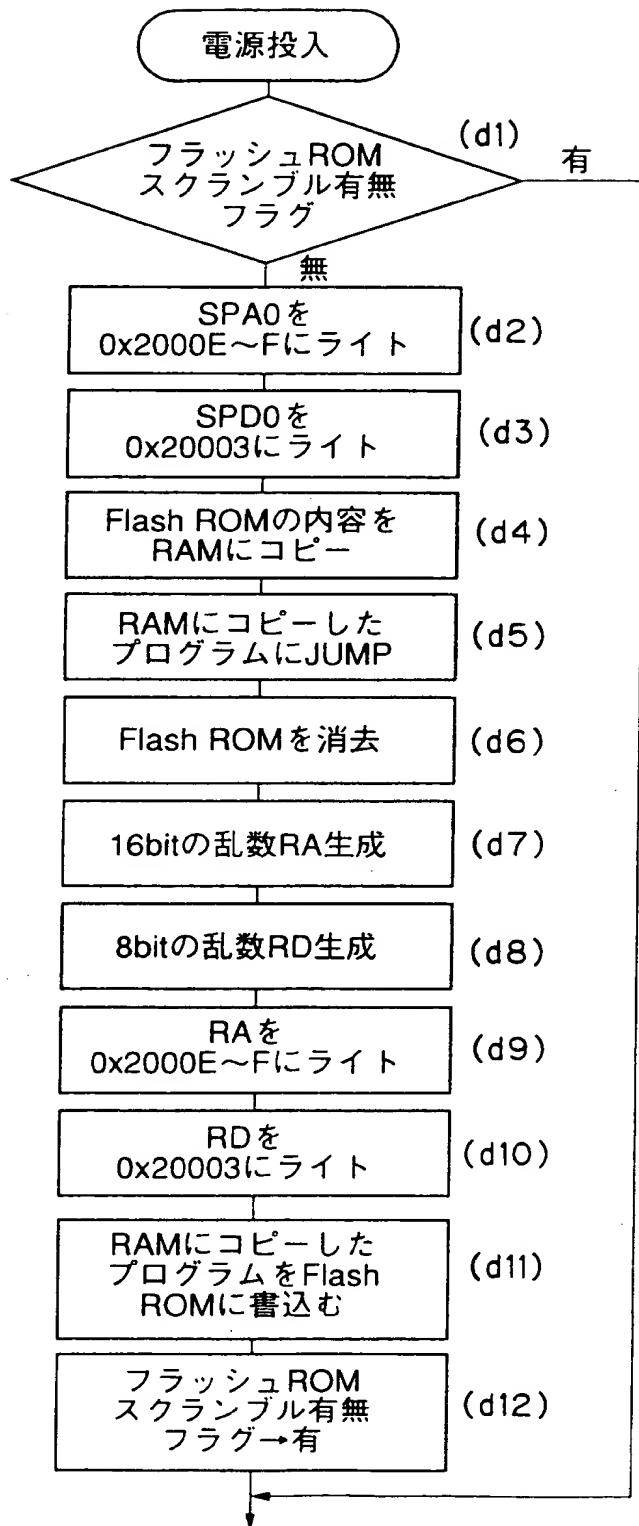
【図 1 4】



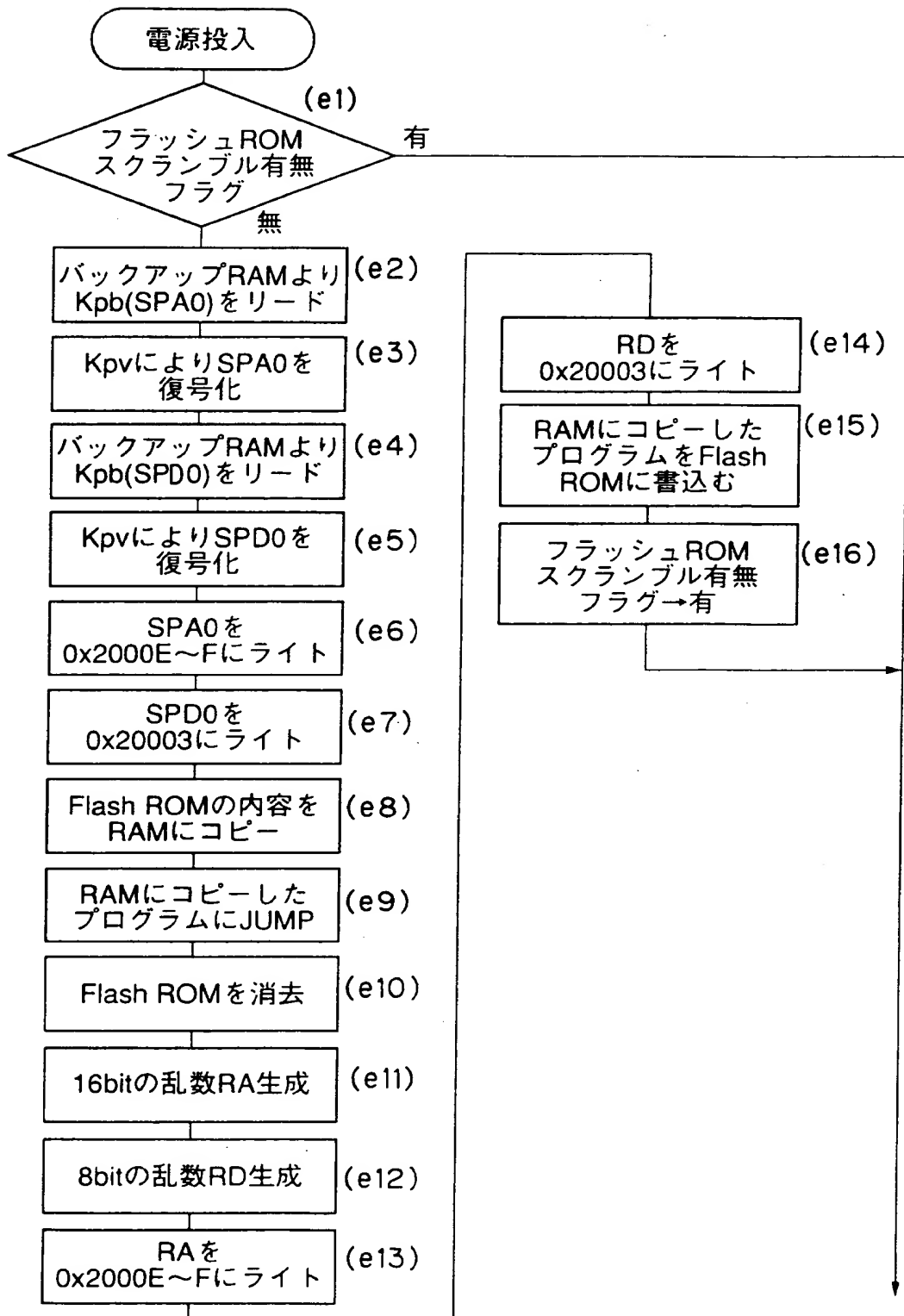
【図 1 5】



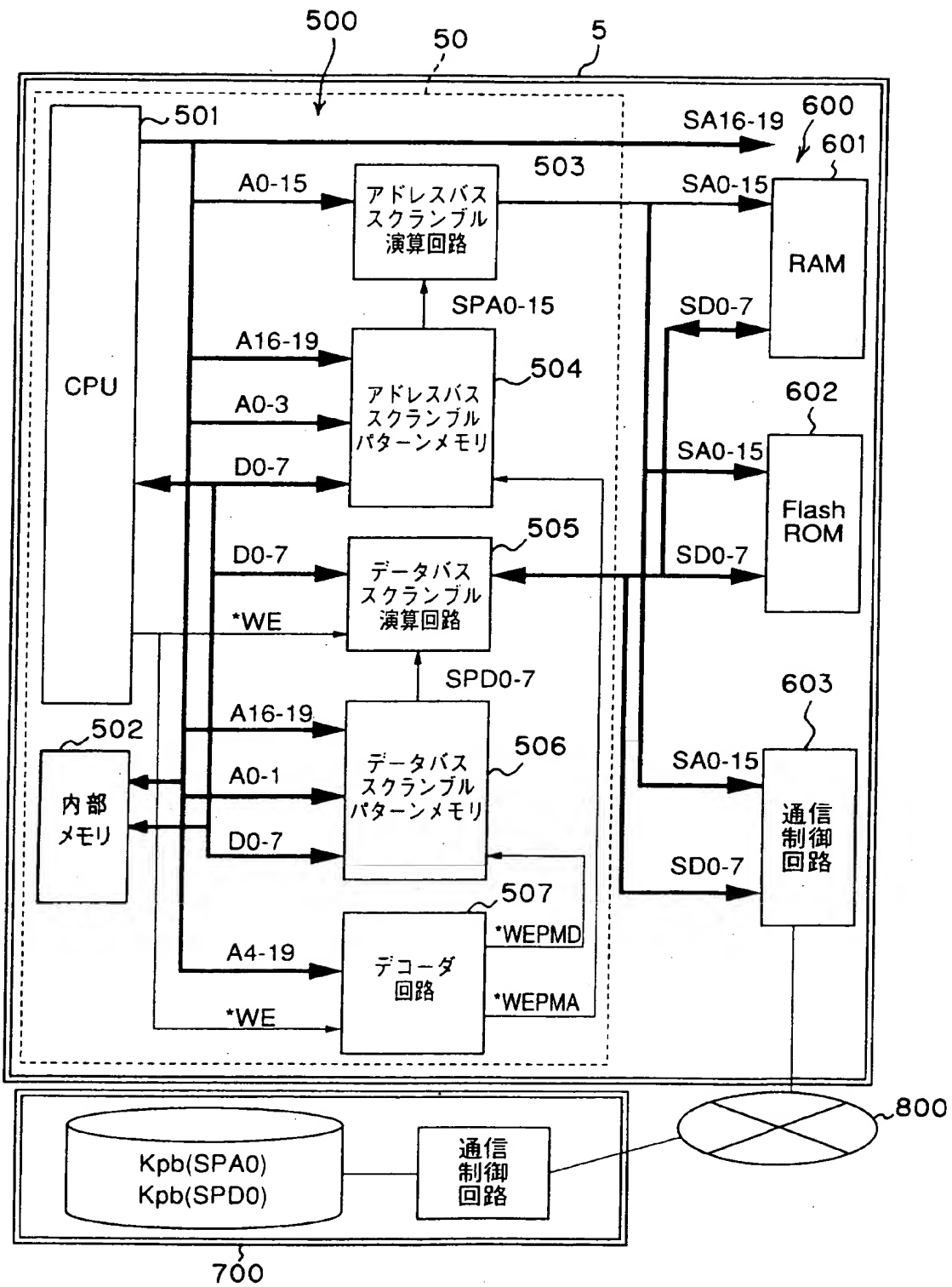
【図 1 6】



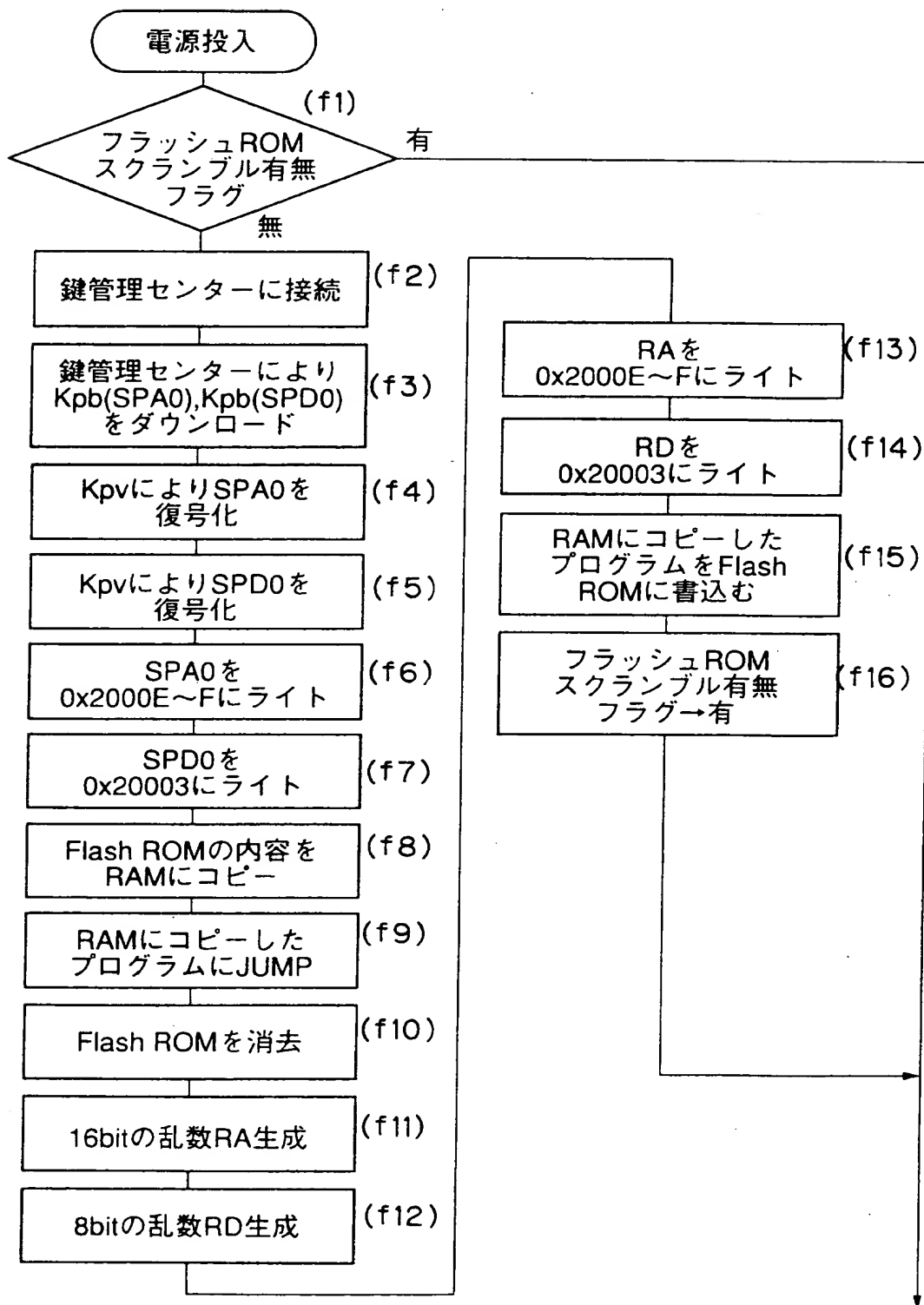
【図 1 7】



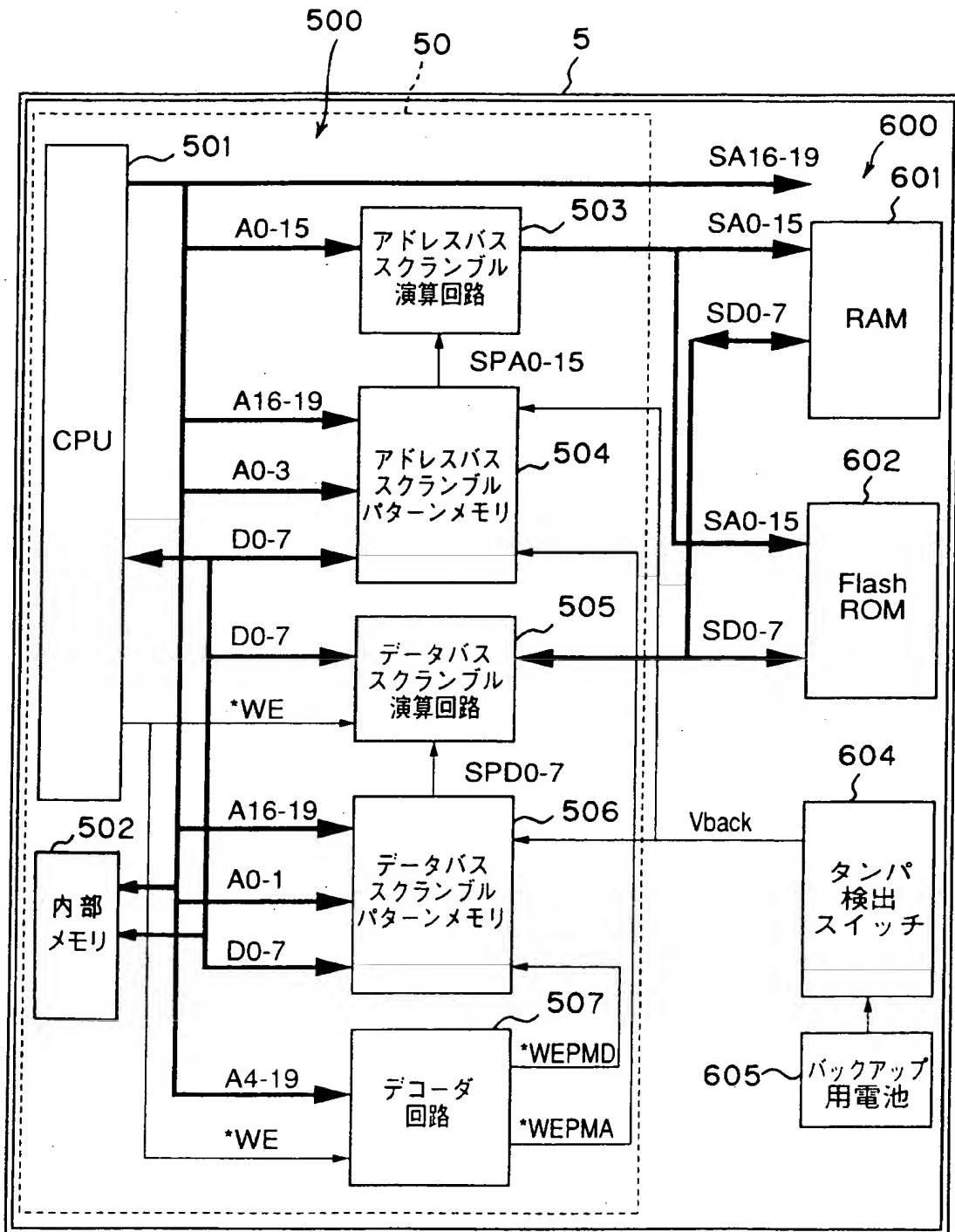
【図18】



【図 19】



【図20】



【書類名】 要約書

【要約】

【課題】本発明は、CPUおよび内部デバイスを有する内部回路と、その内部回路に対し外付けされた外部デバイスを含む外部回路とを備えた処理装置等に関し、不正なアクセスや逆解析の防止を図る。

【解決手段】CPU101と、内部デバイス102～105と、CPU101と内部デバイス102～105とを結ぶとともに外部にまで延びるバスライン110とを含む内部回路100、および、バスライン110の、外部に延びた部分110aに外付けされた外部デバイス201～203，211～212を含む外部回路200を備え、内部回路100が、バスライン110の、外部への出入口に介在し、そのバスライン上のアドレスおよびデータを、外部デバイス全体に割り当てられたアドレス空間を複数に分けた各領域に応じた各暗号化パターンで暗号化する暗号化部120を含む。

【選択図】 図1

出 願 人 履 歴 情 報

識別番号 [000005223]

1. 変更年月日 1996年 3月26日
[変更理由] 住所変更
住 所 神奈川県川崎市中原区上小田中4丁目1番1号
氏 名 富士通株式会社